ASSOCIATION OF
LITHUANIAN BANKS

GUIDELINES
ON
CUSTOMER DUE DILIGENCE

June, 2020

INTRODUCTORY REMARKS

The mission of Association of Lithuanian Banks (the **Association**) is to create a benefit for society by developing a constructive relationship based on mutual understanding and trust between the customers, supervisory institutions and banks. The Association believes that the effective anti-money laundering and counter-terrorist financing policy is essential to achieve this goal. In the year 2020, the Association[1] has prepared the Guidelines on Customer Due Diligence (**Guidelines**) in order to ensure the uniform application of the customer due diligence requirements among the members of the Association.

The Guidelines were prepared in accordance to the European Union and Lithuanian legal acts, the standards of the Financial Action Task Force (**FATF**), best international and European market practices, the best market practices of the LBA members, and in consultation with the Bank of Lithuania and the Financial Crime Investigation Service under the Ministry of Interior of the Republic of Lithuania.

Target audience. The target audience of the Guidelines is first and foremost the members of the Association, in particular, banks, specialised banks, and credit unions. However, the Guidelines should serve as a useful point of reference for other financial institutions and obliged entities, their customers, supervisory institutions and other stakeholders.

Status. The Guidelines are mandatory for the members of the Association. The Guidelines are issued by the Association and therefore cannot be considered as legally binding, although it was prepared in coordination with the Bank of Lithuania and the Financial Crime Investigation Service under the Ministry of Interior of the Republic of Lit huania. The Guidelines provide the basis upon which the members of the Association develop the customer due diligence processes, procedures and technological solutions.

The Guidelines will be amended from time to time to ensure they stay relevant and up-to-date.

[1] On behalf of the Association, the members of the working group: Lina Kavarzaitė, Urtė Armonaitė, Jurgita Nikita, Andrius Merkelis, Edvardas Gudaitis, Tomas Kakanauskas, Augustas Klezys, Aidas Budrys, Vytautas Danta.

DEFINITIONS

Basic Payment Account	A payment account with basic features as provided for in Article 71(1) of the Law on Payments of the Republic of Lithuania.
Beneficial Owner	A natural person who is the owner of the Customer (a legal entity or a foreign undertaking) or controls the Customer and/or the natural person on whose behalf a transaction or activity is being conducted. The Beneficial owner is: 1. in the case of a legal entity: a) the natural person who owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than public companies listed on a regulated market that are subject to the requirements for the disclosure of the business-related information consistent with the EU legislation or subject to equivalent international standards, or through control via other means. A shareholding of 25% plus one share or an ownership interest of more than 25% in the Customer held by a natural person is an indication of direct ownership. A shareholding of 25% plus one share or an ownership interest of more than 25% in the Customer held by a corporate entity, which is under the control of a natural person, or by multiple corporate entities, which are under the control of the same natural person, is an indication of indirect ownership; b) the natural person who holds the position of senior manager of a Customer if no person under point 1(a) above is identified, or if there is any doubt that the person identified is the Beneficial Owner, and after having exhausted all reasonable and proportionate means, 2. in the case of trusts: a) the settlor; b) the trustee; c) the protector, if any; d) the natural person deriving benefit from a legal entity or an entity without legal personality or, if such person is not yet identified, the group of persons in whose main interest the legal entity or an entity without legal personality is set up or operates; e) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means; 3. in the case of a legal entity which administers and allocates funds, and legal arrangements similar to trusts, the natural person holding equivalent position to that referred to in point 2 above.
Business Relationship	Business, professional or commercial relationship of a Customer and the Firm which is connected with their professional activities and which is expected, at the time when the contact is established, to have an element of duration for a certain period (e.g. conclusion of an agreement between the Customer and the Firm, continuous performance of monetary operations and transactions).

Close Associate	1. A natural person who, together with the Politically Exposed Person, is a member of the same legal entity or of a body without legal personality or maintains other business relationship; 2. A natural person who is the only Beneficial Owner of the legal entity or a body without legal personality set up or operating *de facto* with the aim of acquiring property or another personal benefit for the Politically Exposed Person.
Close Family Members	The spouse, the person with whom partnership has been registered (i.e. the cohabitant), parents, brothers, sisters, children and children's spouses, children's cohabitants.
Correspondent Relationship	1. The provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services; 2. The relationships between and among financial institutions, including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.
Customer	A person performing Occasional Transactions adhering to the criteria in specified in paragraph 1.6 or a person who has entered into Business Relationship with the Firm.
Customer Due Diligence	Identification of the Customer and verification the Customer's identity on the basis of documents, data or information obtained from a reliable and independent source; identification of the Beneficial Owner and taking reasonable measures to verify that person's identity so that the Firm is satisfied that they know who the Beneficial Owner is; assessment and, as appropriate, obtainment of information on the purpose and intended nature of the Business Relationship; the conducting of ongoing monitoring of the Business Relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Firm's knowledge of the Customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.
European Supervisory Authorities	European Banking Authority, European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority.
Financial Institutions	1. Credit institutions and financial undertakings as defined by the Law on Financial Institutions of the Republic of Lithuania; 2. Payment institutions as defined by the Law on Payment Institutions of the Republic of Lithuania; 3. Electronic money institutions as defined by the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania; 4. Currency exchange operators as defined by the Law on Currency Exchange Operators of the Republic of Lithuania; 5. Crowdfunding platform operators as defined by the Law on Crowdfunding of the Republic of Lithuania;

	6. Peer-to-peer lending platform operators as defined by the Law on Consumer Credit of the Republic of Lithuania and the Law on the Real Estate-Related Credit of the Republic of Lithuania; 7. Insurance undertakings engaged in life insurance activities and insurance brokerage firms engaged in insurance mediation activities related to life insurance as defined by the Law on Insurance of the Republic of Lithuania; 8. Investment companies with variable capital and collective investment undertakings intended for informed investors and the management undertakings which exercise exclusive control over such entities; 9. Branches of the above-mentioned foreign entities incorporated in Lithuania; 10. Electronic money institutions and payment institutions based in another EU/EEA Member State which provide services in Lithuania through intermediaries, natural persons or legal entities.
Firm	A bank, specialised bank, credit union which is a member of the Association or another financial undertaking which commits to comply with these Guidelines.
Identification	A part of Customer Due Diligence described in paragraphs 4.2 and 4.8. allowing to ascertain the identity of a person on the basis of the personalised unique information directly related to that person.
International Legal Standards / Practices	International legal standards and best practices which, together with the applicable legal acts, were used to create these Guidelines and comprising of the following documents: 1. Guidance on the Correspondent Banking Services issued by the Financial Action Task Force dated October 2016; 2. Guidance on Transparency and Beneficial Ownership issued by the Financial Action Task Force dated 27 October 2014; 3. Guidance on the Politically Exposed Persons issued by the Financial Action Task Force dated June 2013; 4. Guidance for the UK Financial Sector on Prevention of Money Laundering/ Combating Terrorist Financing adopted by the Joint Money Laundering Steering Group dated June 2017 and amended 13 December 2017 (as amended and supplemented from time to time); 5. other international legal standards and best practices of the members of the Association.
JADIS Regulations	Regulations of the Information System of Legal Entities Participants approved by the Order of the Minister of Justice of the Republic of Lithuania No. 1R-231 dated 11 October 2013 (as amended and supplemented from time to time).
Law	Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania.
Lithuanian Civil Code	Civil Code of the Republic of Lithuania.

Money Laundering	1. The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action; 2. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity; 3. The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity; 4. Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points 1, 2 and 3.
Multi-Level Ownership Structure	An ownership structure where at least one of the shareholders of the Customer is a legal person, a legal arrangement or a body without legal personality.
Obliged Entities	Financial Institutions and Other Obliged Entities subject to the AML / CFT requirements.
Occasional Transaction	A transaction that is not carried out as part of a Business Relationship.
Other Obliged Entities	1. Auditors that engage in auditing activities individually, or audit firms; 2. Bailiffs and their representatives; 3. Undertakings providing accounting or tax advisory services and persons providing such services individually, and any other person that undertakes to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters as principal business or professional activity; 4. Notaries, notary's representatives and other persons entitled to perform notarial actions, as well as attorneys and assistant attorneys, when acting on behalf of and for the Customer and when assisting the Customer in the planning or execution of transactions for their Customer concerning the purchase or sale of real property or business entities, management of Customer money, securities or other property, opening or management of bank or securities accounts, organisation of contributions necessary for the establishment, operation or management of legal entities or other organisations, emergence or creation, operation or management of trust or company forming and administration service providers and/or related transactions; 5. Providers of the services of trust or company forming or administration not covered under points 1, 3 and 4 above; 6. Persons engaged in economic and commercial activities covering trade in precious stones, precious metals, items of movable cultural property, antiques or other property the value whereof is equal to or exceeds EUR 10,000 or an equivalent amount in foreign currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked, to the extent that payments are made in cash, except in cases provided in points 12 and 13 of this paragraph;

7. Companies organising gambling or lotteries;
8. Close-ended investment companies;
9. Real estate agents (brokers), when acting on behalf of and for their Customer and when assisting their Customer in the performance of transactions on sale and purchase of real estate and/or related operations, including when acting as intermediaries in the letting of immovable property, but only in relation to transactions for which the monthly rent amounts to EUR 10 000 or more, or an equivalent amount in foreign currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
10. Virtual currency exchange operators;
11. Custodian wallet providers;
12. Persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more, or an equivalent amount in foreign currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
13. Persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports established in line with the Regulation (EU) No 952/2013 of the European Parliament and of the Council Regulation of 9 October 2013 laying down the Union Customs Code (OJ 2013 L 269, p. 1), as last amended by the Regulation (EU) No 2019/632 of the European Parliament and of the Council Regulation of 17 April 2019 (OJ 2019 L 111, p. 54), where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more, or an equivalent amount in foreign currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

Politically Exposed Person

Natural persons who are or have been entrusted with Prominent Public Functions and Close Family Members or Close Associates of such persons.

Prominent Public Functions

1. The head of the state, the head of the government, a minister, a vice-minister or a deputy minister, a secretary of the state, a chancellor of the parliament, government or a ministry;
2. A member of the parliament;
3. A member of the Supreme Court, the Constitutional Court or any other supreme judicial authorities whose decisions are not subject to appeal;
4. A mayor of the municipality, a head of the municipal administration;
5. A member of the management body of the supreme institution of state audit or control, or a chair, deputy chair or a member of the board of the central bank;
6. Ambassadors of foreign states, a *chargé d'affaires ad interim*, the head of the Lithuanian armed forces, commander of the armed forces and units, chief of defence staff or senior officer of foreign armed forces;

	7. A member of the management or supervisory body of a public undertaking, a public limited company or a private limited company, whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state; 8. A member of the management or supervisory body of a municipal undertaking, a public limited company or a private limited company whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state, and which are considered as large enterprises in terms of the Law on Financial Statements of Entities of the Republic of Lithuania; 9. A director, a deputy director or a member of the management or supervisory body of an international intergovernmental organisation; 10. A leader, a deputy leader or a member of the management body of a political party.
Risk Factors Guidelines	Joint Guidelines No. JC 2017 37 under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions dated 4 January 2018 (as amended and supplemented from time to time) issued by the European Supervisory Authorities.
Senior Manager	An official or an employee holding a significantly high position and having considerable knowledge about the exposure of the Firm to money laundering and/or terrorist financing risk, and responsible for the adoption of the decisions that may have an impact on such risk.
Shell Bank	A credit institution or an institution that carries out activities equivalent to those carried out by a financial institution, incorporated in a jurisdiction in which it has no physical presence, has no actually functioning management or organisational structure and internal control systems, and is unaffiliated with a financial group regulated by competent authorities.
Technical Requirements	Technical Requirements for Remote Customer Identification by Electronic Means Enabling Video-Streaming approved by the Order No. V-314 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania on 30 November 2016 (as amended and supplemented from time to time).
Terrorist Financing	Provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Article 2 of the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999.
Third Party	A Financial Institution or Other Obliged Entity supervised by competent authorities, or a Financial Institution or Other Obliged Entity registered in another EU/EEA Member State or a state which is a third country, and meeting the following requirements: a) it is subject to mandatory professional registration, recognised by law; b) it is registered in an EU/EEA Member State or in a third country which applies requirements that are equivalent to the EU-established Customer and Beneficial Owner identification and record keeping requirements, and which is supervised by the competent authorities in terms of the compliance with the said requirements.

ABBREVIATIONS

AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
AMLD4	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 (or the 4th AML Directive).
AMLD5	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (or the 5th AML Directive).
BO	Beneficial Owner
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
EEA	European Economic Area
ESAs	European Supervisory Authorities
EU	European Union
EU/EEA	European Union and European Economic Area
FATF	The Financial Action Task Force
FIU	Financial Intelligence Unit
ML/TF	Money Laundering and Terrorist Financing
PEP	Politically Exposed Person
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report

INTRODUCTION

The Law requires a Firm to identify, assess and mitigate the ML/TF and other financial crime risks. Furthermore, it requires in accordance with the identified risks, nature and size of the Firm to establish procedures and systems aimed to assess, manage and mitigate ML/TF risks to which the Firm is exposed to.

The identification, assessment, understanding and mitigation of the risks of ML/TF affecting the Firm are the core elements of the risk-based approach which, according to the nature of FATF Recommendations, AMLD4 and AMLD5, is at the centre of the AML/CFT framework. FATF and AMLD4 recognize that ML/TF risks can vary depending on the nature and the size of the Firm, therefore, AML/CFT measures must be proportionate to the degree of those risks.

For the Firm, CDD is one of the main AML/CFT measures and is crucial in the process of identification, assessment and mitigation of ML/TF risks. CDD helps the Firm understand whether Customers are who they say they are and enables them to assist FIU and other competent authorities by providing information about suspicious activity which are being investigated. CDD includes:

1. identifying the Customer and verifying the Customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
2. identifying the BO and taking reasonable measures to verify that person's identity so that the Firm is satisfied that they know who the BO is;
3. assessing and, as appropriate, obtaining information on the purpose and intended nature of the Business Relationship; and
4. conducting ongoing monitoring of the Business Relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Firm's knowledge of the Customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

A. THE TIMING AND IMPLICATIONS OF CDD

1. General Information

1.1. The Firm should perform CDD on all its Customers that establish a Business Relationship or perform an Occasional Transactions adhering to the criteria specified in paragraph 1.6 with the Firm irrespective of the Firm's product or service that the Customer is using. E.g. CDD must be performed for the Customers seeking to open a payment or a bank account with the Firm; for Customers seeking to obtain a loan from the Firm; Customers using the leasing products offered by the Firm, etc.

1.2. Where there are several parties involved, not all of them should be considered as Customers. E.g. in a financing transaction, a surety provider under a suretyship agreement providing a surety to secure the obligations of the Customer arising from the transaction documents would not be considered as the Customer of the Firm unless the surety provider is using other services of the Firm for which the surety would be considered as a Customer of the Firm (e.g. has a bank account with the Firm).

1.3. In these situations the Firm should still perform Identification of a party to a transaction documentation which is not considered a Customer. However, in case the Firm deems it necessary, the Firm may collect additional information on the party referred to in paragraph 1.2 who is not considered a Customer (e.g. establish its source of funds). It may be relevant in situations where such a party is, e.g., a surety, which may be held liable to the Firm and be required to settle the debts of the Customer in case the Customer fails to fulfil its obligations to the Firm.

1.4. In case the circumstances change in a way that such a party becomes a Customer of the Firm, the full CDD has to be performed.

1.5. In light of the above, for the purpose of the AML/CFT regulation, a person whom the Firm provides its professional and/or financial services to should be considered as the Customer of the Firm.

Article 9(1) of the Law

1.6. CDD should be performed for the following Occasional Transactions:

1. a single operation or several operations which appear to be linked or transactions the value whereof equals or exceeds EUR 15,000 or an equivalent amount in foreign currency;
2. currency exchange operations (buying or selling currency) in cash, where the amount of cash being acquired or sold amounts to or exceeds EUR 3,000 or an equivalent amount in foreign currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
3. money remittance services in cash, where the sum of money sent or received exceeds EUR 600 or an equivalent amount in foreign currency;
4. money transfers in compliance with the provisions of Regulation (EC) No. 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006;
5. virtual currency exchange operations or transactions in virtual currency the value whereof equals or exceeds EUR 1,000 or an equivalent amount in foreign or virtual currency, or before depositing or withdrawing virtual currency amounting to or above EUR 1,000 or an equivalent amount in foreign or virtual currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked (the value of the virtual currency is determined at the time of the monetary operation or transaction), unless the Customer and BO have already been identified.

	1.7.	For the purposes of effective ongoing monitoring of the Business Relationship and Occasional Transactions referred to in paragraph 1.6 and timely determination of the several related monetary operations or transactions, the Firm has to perform Identification on the payer and the payee carrying out the transaction, and screen the payer and the payee against the relevant financial sanctions list even where the transaction is performed below the thresholds referred to in paragraph 1.6 above.
International Legal Standards / Practices	1.8.	**Electronic Verification** For the purposes of effective ongoing monitoring of the Business Relationship and Occasional Transactions referred to in paragraph 1.6 and timely determination of the several related monetary operations or transactions, the Firm has to perform Identification on the payer and the payee carrying out the transaction, and screen the payer and the payee against the relevant financial sanctions list even where the transaction is performed below the thresholds referred to in paragraph 1.6 above.
International Legal Standards / Practices	1.9.	Before using the services of a company for electronic verification the Firm must be satisfied that information provided by such a company is considered to be sufficiently extensive, reliable and accurate, and independent of the Customer. The Firm should, therefore, consider whether such a company meets at least the following criteria: 1. the company uses a range of multiple, positive information sources, including other activity history where appropriate; 2. it is accredited, or certified, to offer the identity verification service through a governmental, industry or trade association process that involves meeting minimum published standards; 3. it accesses negative information sources, such as databases relating to identity fraud; 4. it accesses a wide range of alert data sources; 5. its published standards, or those of the scheme under which it is accredited or certified, require its verified data or information to be kept up to date, or maintained within defined periods of re-verification; 6. arrangements exist whereby the company's continuing compliance with the minimum published standards is assessed; 7. the company has transparent processes that enable the Firm to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.
International Legal Standards / Practices	1.10.	The company providing electronic verification should also have processes that allow the Firm to record and store the information they used to verify an identity.

2. The Timing of CDD

Article 9(12) of the Law	2.1.	The CDD measures applied by the Firm must be extensive, targeted and proportionate in order to identify if Customers are acting in their own name and benefit, identify the BO and in the cases where the Customer is acting through a representative – also identify the representative.

Article 9(1) of the Law

The Firm must apply CDD measures when they do any of the following:

1. establish a Business Relationship;
2. carry out Occasional Transactions referred to in paragraph 1.6;
3. where there are doubts about the veracity or authenticity of the previously obtained identification data of the Customer and BO;
4. in any other case where there are suspicions that the act of ML/TF is, was or will be performed.

The Business Relationship or Occasional Transaction referred to in paragraph 1.6 can only commence after the Firm has duly performed at least the following actions:

1. Identified the Customer and verified its identity;
2. Identified the BO and verified its identity;
3. Determined the purpose and intended nature of the Business Relationship;
4. Assessed the ML/TF risk of the Customer and allocated the Customer to an appropriate risk category;
5. Made sure there are no grounds to apply EDD (including screening the relevant persons against PEP lists), and applied EDD in case necessary;
6. Screened the relevant persons against the relevant financial sanctions list.

General rule for the timing of CDD

Article 9(1) of the Law 2.3. The CDD actions listed in paragraph 2.2 above must, subject to the exceptions referred to below, be completed before the establishment of a Business Relationship or carrying out of an Occasional Transaction adhering to the criteria specified in paragraph 1.6.

Exception in case of low ML/TF risk

Article 9(5) of the Law 2.4. When opening accounts, the verification of the Customer's identity can be completed as soon as possible, but no later than 1 month after the Customer approaches the Firm in order to establish a Business Relationship.

The Firm can open account for a Customer before completing CDD if all conditions are met:

1. A low ML/TF risk is established;
2. Identification information foreseen in paragraph 4.2 points 1-4, paragraph 4.8 and paragraph 6.18 of these Guidelines is collected;
3. It is ensured that the CDD is completed within 1 month after the account is opened;
4. The Customer is not be able to perform any transactions in the account before completing the CDD.

E.g. in cases where credit or debit cards are ordered from the Firm, an account may be opened and a card can be ordered and manufactured in advance, while the Customer's identity can be verified as soon as possible, but no later than within 1 month, either physically or using non-face-to-face identification tools that are in line with the legal requirements.

Article 9(5) of the Law 2.5. The Firm must establish their internal policy and internal control procedures related to the management of the risk arising as a result of the opening of accounts without verifying the Customer and BO's identity.

3. The Implications of CDD

Article 9(22) of the Law 3.1. If during the CDD of the Customer, the Firm becomes suspicious that ML/TF is being conducted, and further identification procedures of the Customer and BO might raise suspicions to the Customer that the information about the Customer may be submitted to competent authorities, the Firm may not proceed with the CDD process of the Customer and BO and not enter into the Business Relationship or perform an Occasional Transaction adhering to the criteria of paragraph 1.6 with the Customer. In such cases the information has to be submitted to the FIU.

Article 9(18) of the Law, International Legal Standards / Practices 3.2. Where the Firm is unable to apply CDD measures due to the fact that:

1. the Customer fails to submit the required data and is unresponsive;
2. the Customer submits incomplete data or if the data is incorrect;
3. the Customer or its representative avoids submitting the data required for establishing its identity, conceals the identity of the BO or avoids submitting the information required for establishing the identity of the BO, or the submitted data is insufficient for this purpose;
4. the Firm cannot ensure the performance of the following requirements:
   a) determine whether the Customer operates on own behalf or is controlled;
   b) establish the identity of the BO,
   c) establish the identity of the Customer's representative, if required;
   d) understand the ownership and control structure and the nature of business of the Customer (legal entity);
   e) obtain the information about the purpose and intended nature of the Customer's Business Relationship;
   f) verify the identity of the Customer and the BO according to the documents, data or information obtained from a reliable and independent source;
   g) conduct the ongoing monitoring of the Customer's Business Relationship, transactions performed during the course of Business Relationship and Occasional Transactions;
   h) comply with the other requirement to apply the CDD or EDD measures,

the Firm:

1. is prohibited from carrying out a transaction through a bank account with or on behalf of the Customer;
2. is prohibited from engaging in a Business Relationship or carrying out an Occasional Transaction adhering to the criteria in paragraph 1.6 with the Customer;
3. is prohibited from continuing the Business Relationship with the Customer;
4. after having assessed the risk of the ML/TF, must consider whether it ought to be making an STR.

Article 9(21) of the Law	3.3.	It is prohibited for the Firm to issue anonymous passbooks, open anonymous accounts or accounts in an obviously fictitious name, rent anonymous safe-deposit boxes, open accounts or entering into Business Relationship without requesting the Customer to submit the data confirming their identity or when there is a substantiated suspicion that the data recorded in these documents are false or fraudulent.
		Refusal to On-board / Termination of a Business Relationship or Occasional Transactions
	3.4.	In case of a new Customer, where the Firm is unable to fulfil its CDD obligations (e.g. verify the Customer's identity) because the data or documents allowing the Identification and/or verification of a Customer or BO's identity, or determination of a purpose and intended nature of the Business Relationship or Occasional Transactions adhering to the criteria in paragraph 1.6 cannot be obtained due to the fact that: 1. the Customer is uncooperative and/or does not provide the requested data or information necessary to perform CDD; and/or 2. there are no relevant reliable and independent sources to verify the information provided by the Customer, the Firm must duly assess the ML/TF risk and take appropriate measures to mitigate such risk which may include the refusal to on-board such a Customer or perform the Occasional Transaction adhering to the criteria in paragraph 1.6.
	3.5.	In case of the existing Customers, where the Firm is unable to duly perform its CDD obligations as described in paragraph 3.4 above, the Firm must also assess the ML/TF risk and take appropriate measures to mitigate such risk. Such measures may include suspension of the monetary operations or transactions performed by such a Customer until the Customer provides the information and/or documents necessary for the CDD. The Firm should also assess whether the Business Relationship should be terminated / the Occasional Transaction adhering to the criteria in paragraph 1.6 should not be performed, and/or an STR should be made if: 1. the Customer whose monetary operations or transactions were suspended (or other appropriate measures were applied) does not fulfil the requirements to provide the necessary information and/or documents during a proportionate period of time; and/or 2. there are no relevant reliable and independent sources to verify the information provided by the Customer.
International Legal Standards / Practices	3.6.	The termination of the Business Relationship or Occasional Transaction adhering to the criteria specified in paragraph 1.6 should be taken only if it is proportionate and should be possible only after the other appropriate measures are exhausted and the Firm is still unable to comply with the AML/CFT requirements.

ML/TF Risk Scoring of the Customer

3.7. The Firm has to assess the ML/TF risk of each Customer and score the Customer before establishing a Business Relationship and/or before the Customers perform an Occasional Transaction adhering to the criteria in paragraph 1.6. Only after the ML/TF risks of a particular Customer are assessed and the Customer is allocated to an appropriate score category, the Firm can decide whether there are grounds to apply SDD, or whether EDD measures, in addition to the CDD measures, must be applied, and the extent of such measures.

3.8. The Business Relationship and Occasional Transactions adhering to the criteria in 1.6 must be assessed from the perspective of at least the following risk factors:

1. Customer risk;
2. Products, services and transactions and their delivery channels risk;
3. Countries and geographical areas risk.

3.9. Following its risk assessment, the Firm should categorise the Business Relationships and Occasional Transactions adhering to the criteria in 1.6 according to the perceived level of ML/TF risk.

Risk Factors Guidelines, International Legal Standards / Practices

3.10. The Firm should decide on the most appropriate way to categorise risk. This should depend on the nature and size of the Firm's business and the types of ML/TF risk it is exposed to. However, all Firms should have at least 3 levels of categories: e.g. high, standard (medium) and low. More detailed categorisations are also possible. It is also possible that the Firm decides not to apply SDD to the low risk Customers, and instead applies CDD as if for the standard risk Customers.

3.11. After completing the CDD, all Business Relationships or Occasional Transactions adhering to the criteria in paragraph 1.6 must be allocated to one of the categories. There should not be any situations where a Business Relationship or Occasional Transaction adhering to the criteria in paragraph 1.6 is not allocated to any of the risk categories.

Risk Factors Guidelines

3.12. When weighting the risk factors associated with a Business Relationship or Occasional Transactions adhering to the criteria in paragraph 1.6, the Firm should make an informed judgement about the relevance of different risk factors in the context of a Business Relationship or Occasional Transaction adhering to the criteria in paragraph 1.6. This often results in the Firm allocating different "scores" to different factors; e.g. the Firm may decide that a Customer's personal links to a jurisdiction associated with higher ML/TF risk is less relevant in light of the features of the product they seek.

Risk Factors Guidelines

3.13. Ultimately, the weight given to each of these factors is likely to vary from product to product and Customer to Customer (or category of Customer) and from one Firm to another. When weighting risk factors, the Firm should ensure that:

1. weighting is not unduly influenced by just one factor;
2. economic or profit considerations do not influence the risk rating;
3. weighting does not lead to a situation where it is impossible for any Business Relationship or Occasional Transactions adhering to the criteria in paragraph 1.6 to be classified as high risk;

4. the provisions of AMLD4, AMLD5 and national laws regarding situations that always present a high money laundering risk cannot be over-ruled by the Firm's weighting; and
5. they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately.

Risk Factors Guidelines

Where a Firm uses automated systems to allocate overall risk scores to categorise Business Relationship or Occasional Transactions adhering to the criteria in paragraph 1.6 and does not develop these in-house but purchases them from an external provider, it should understand how the system works and how it combines risk factors to achieve an overall risk score. The Firm must always be able to satisfy itself that the scores allocated reflect the Firm's understanding of ML/TF risk and it should be able to demonstrate this to the competent authority.

The Firm must ensure that, in case required, the Customer's risk category is duly updated and the actions related thereto are performed taking into account information provided in sections 17 and 18 of these Guidelines.

Implementation of the Sanctions Regime

3.16. The Firm is obliged to comply with the national, EU and United Nations sanctions regime in accordance to the Law on the Implementation of Economic and Other Sanctions of the Republic of Lithuania and its implementing legal acts, in particular, with the Instructions on the Supervision of the Appropriate Implementation of International Financial Sanctions in the Field of Regulation of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic Of Lithuania approved by the Order No. V-273 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania dated 20 October 2016 (as amended and supplemented from time to time).

International Legal Standards / Practices

3.17. Before establishing a Business Relationship or performing an Occasional Transactions, the Firm must screen the Customer, the person performing the Occasional Transactions, the Customer's representative, the persons that make up the Customer's ownership structure and its BO against the relevant sanctions lists. When the Customer performs a monetary operation or transaction as a part of the Business Relationship or performs Occasional Transactions, the Firm must screen both parties of the monetary operation or transaction, as well as screen the other payment details (in case a payment is made), against the sanctions lists.

International Legal Standards / Practices

3.18. The relevant parties referred to in paragraph 3.17 above must be screened against the relevant sanctions list not only upon the on-boarding of the Customer, but the Firm's Customer base should also be periodically, at least every day, screened against the relevant sanctions list to ensure the correct implementation thereof. The screening of the Customer base must include the screening of the Customer, its representative, the persons that make up the Customer's ownership structure and the BO.

International Legal Standards / Practices	3.19.	The Firm must screen the relevant parties against at least the following sanctions list: 1. The consolidated list of individuals, groups and entities subject to EU financial sanctions; 1. The United Nations Security Council sanctions list; 2. The Office of Foreign Assets Control (OFAC) sanctions list.
International Legal Standards / Practices	3.20.	Where the Firm chooses to use automated checks for the sanctions screening, they should ensure that relevant software includes checks against the lists relevant to the Firm and that such lists are kept up to date.

B. IDENTIFICATION OF THE CUSTOMER AND VERIFICATION OF THE CUSTOMER'S IDENTITY

4. Identification and Verification of the Customer's Identity

		Identification and Verification of Natural Persons
	4.1.	In general, identification of the Customer is a part of CDD allowing to ascertain the identity of a person on the basis of the personalised unique information directly related to that person. Verification means verifying such information from the documents or data obtained from a reliable and independent source.
Article 10(1) of the Law	4.2.	In identifying the Customer (natural person), the Firm has to obtain the following data: 1. name(s); 2. surname(s); 3. personal identification number (in the case of foreigners – the date of birth (if any – personal identification number or other unique sequence of symbols assigned to the person for identification purposes, the number and validity term of the residence permit in the Republic of Lithuania, place and date of its issue (applicable to foreigners)); 4. photo; 5. signature (unless it is not necessary in the identification document); 6. citizenship (in the case of a stateless person – the country where the personal identity document was issued).
	4.3.	Subject to paragraph 4.19, to verify the above information the Firm must obtain the appropriate personal identification documents. Passport, personal identification card, diplomatic passport, temporary or permanent residence permit in Lithuania should be considered as appropriate identification documents of the Customer (natural person).
	4.4.	In case the personal identification document is obtained from the Customer, the Customer (natural person) should present a valid personal identification document.
Article 10(3) of the Law	4.5.	Where the Customer (natural person) is represented by another natural person, the identity of such a representative has to be established in the same manner as applied to the Customer (natural person).

Article 10(5) of the Law	4.6.	The Customer (natural person's) representative has to provide a document evidencing the authorisation and the Firm has to verify: 1. the validity of the document (i.e. the right of the issuing person to issue such authorisation); 2. the date of expiry of the authorisation; 3. the actions to be performed under the authorisation.
Article 10(5) of the Law	4.7.	The authorisation has to be in line with the requirements of the Lithuanian Civil Code. Under the Lithuanian Civil Code authorisations (e.g. a Power of Attorney, procuration) issued by natural persons have to be certified by a notary public. The authorisation issued abroad has to be legalised or bear an Apostille.
		Identification and Verification of Legal Persons
Article 10(2) of the Law	4.8..	In identifying the Customer (legal person) the Firm has to obtain the following data on the Customer: 1. name; 2. legal form; 3. registered office address; 4. actual business address; 5. legal code (if any); 6. extract from register and the date of its issuance.
	4.9.	Subject to paragraph 4.19, in order to verify the above information the Firm must obtain the appropriate documents. Normally the data referred to in paragraph 4.8 above is provided for in the extract from the Register of Legal Entities of the Republic of Lithuania or equivalent registers abroad.
Article 10(2) of the Law	4.10.	In case the aforementioned documents are obtained from the Customer itself, they have to be either in an original form or copies certified by a notary public.
Article 10(3) of the Law	4.11.	The Firm also has to obtain information about the manager of the Customer (legal person): 1. name(s); 2. surname(s); 3. personal code. If the manager is a foreign national – date of birth (if available – personal code or any other unique sequence of symbols intended for the identification of a person), 4. citizenship (if the person is stateless – the country which has issued the identification document).
Article 10(4) of the Law	4.12.	The Firm may obtain data or information on the manager of the Customer (legal person) directly from the state information systems or registries and not to require such data or information from the Customer (legal person).
	4.13.	For a Customer (legal person) that is in the process of incorporation but is not yet incorporated, the Firm should require at least original copies of an incorporation act or memorandum of incorporation and, if deemed necessary, a document evidencing the authority of the Customer's representative.
Article 10(3) of the Law	4.14.	Where the Customer (legal person) is represented by a natural person, the identity of such representative has to be established in the same manner as applied to the Customer (natural person).

Article 10(5) of the Law	4.15.	The Customer (legal person's) representative also has to provide a document evidencing the authorisation and the Firm has to verify: 1. the validity of the document (i.e. the right of the issuing person to issue such authorisation); 2. the date of expiry of the authorisation; 3. the actions to be performed under the authorisation.
Article 10(5) of the Law	4.16.	The authorisation has to be in line with the requirements of the Lithuanian Civil Code. The authorisation issued abroad has to be legalised or bear an Apostille. In case the right of representation of the Customer (legal person) is evident from the registry extract, Articles of Association or equivalent documents evidencing the identity of the Customer (legal person), a separate document of authorisation (e.g. a Power of Attorney) should not be required.
		Other Considerations Regarding Verification
Article 9(15), 12(3) of the Law	4.17.	The Firm has the obligation to verify the data, documents and information received form the Customer during the CDD using the documents, data or information obtained from a reliable and independent source.
	4.18.	Verification of the information obtained in the course of identification process means using data from a reliable and independent source (e.g. from documents listed in paragraphs 4.3, 4.9) to confirm that the data collected on the Customer and the BO (e.g. data specified in paragraphs 4.2 and 4.8) are true and correct. This means that the purpose of the verification of information is to ensure that the person who wants to establish a Business Relationship or conclude an Occasional Transaction referred to in paragraph 1.6 is the person they claim to be.
Article 10(4) of the Law	4.19.	The Firm has the right to obtain the documents, data or information necessary for the identification and verification of the Customer and BO's identity directly from the state information systems or registries, and not have to require the Customer to submit such documents, data or information, provided that the data or information obtained directly from the state information systems or registers is certified by the Customer by its signature or advanced or qualified electronic signature. The Customer's signature is not required if: 1. the documents, data or information obtained from state information systems or registers do not differ from the documents, data or information previously approved by the signature of the Customer; 2. documents, data or information have been obtained from the Population Register of the Republic of Lithuania; 3. the documents, data or information obtained from the state information systems or registers are on the manager of the Customer (legal person), as described in paragraph 4.12.
Article 10(5), Article 10(6) of the Law	4.20.	When Identifying and verifying the identity of the Customer and persons performing Occasional Transactions referred to in paragraph 1.6, the Firm must: 1. in case the identification documents are obtained from the Customer, assess whether such documents are valid; establish whether the document produced contains the Customer's photograph; 2. evaluate the condition of the document produced by the Customer (when the Customer is physically present); 3. ascertain whether the natural person or legal entity has necessary powers to act on the Customer's behalf.

Article 10(5), Article 10(6) of the Law 4.21. When Identifying and verifying the identity of the Customer before the establishment of the Business Relationship or before performing Occasional Transactions referred to in paragraph 1.6, the Firm, in addition to the actions referred to in paragraph 4.20, must:

1. in case the identification documents are obtained from the Customer itself, make a copy of such document(s) of a natural person, in particular, copy the pages containing the photograph of the natural person and other data required for Identification purposes, or scan the document (when the Customer is physically present). In case paper copies are made, the Firm must mark each such copy as a "true copy".
2. check whether there are circumstances requiring to apply the EDD, and apply EDD if necessary.

5 Identification and Verification of the Customer when the Customer is Not Physically Present

5.1. General Information

Article 11(1) of the Law 5.1.1. The Customer and BO can be identified and their identities verified without the Customer being physically present for identification in one of the following alternative ways:

1. when using the Third Party information on the Customer and BO;
2. when using the electronic identification means issued in the EU and operating under the electronic identification schemes with the substantial or high assurance levels established in 23 July 2014 Regulation (EU) No. 910/2014;
3. where the identity-related information is approved by the qualified electronic signature using the qualified certificate for electronic signature in line with the requirements of Regulation (EU) No. 910/2014.
4. when using electronic means allowing video-streaming by one of the following methods:
   a) the original of the identification document or the equivalent residence permit in Lithuania is captured through video-streaming and the Customer's identity is confirmed by at least the advanced electronic signature in line with the requirements of Article 26 of Regulation (EU) No. 910/2014; or
   b) the Customer's facial image and the original of the identification document or the equivalent residence permit in Lithuania produced by the Customer are captured by way of video-streaming,
5. in cases where:
   a) before commencing the use of the services of the Firm, a payment order is made to the payment account of the Firm from the account held on behalf of the Customer in the credit institution which is registered in EU/EEA Member State or in a third country which applies the requirements equivalent to the requirements of the Law and which is monitored by competent authorities as to the compliance with such requirements; and

Article 11(1) of the Law

b) a paper copy of the identification document which is certified in the manner prescribed law is submitted. The certification requirements are provided for in the Description on the Certification and Provision of Personal Identity Documents approved by the Order No. V-131 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania on 12 September 2017 (as amended and supplemented from time to time).

Article 11(2) of the Law

5.1.2. The establishment of the identity of a Customer and BO is possible only if all the below listed conditions exist:

1. prior to establishing the identity of the Customer and BO in cases referred to in points 1-3 of paragraph 5.1.1 above, the identity of the Customer had been established in one of the following ways:
   a) by the Third Party with the Customer being physically present; or
   b) by using electronic means enabling video-streaming by one of the methods described in point 4 of paragraph 5.1.1 above; or
   c) or using the method specified in point 5 of paragraph 5.1.1 above; or
   d) when the identity of the Customer had been established with their physical presence when issuing an electronic identification means operating under the electronic identification scheme with the substantial or high assurance levels; or
   e) when the identity of the Customer had been established with their physical presence prior to issuing him a qualified certificate for electronic signature, and
2. the identity of the representative of the Customer and BO was established following the CDD requirements.

This means that in order for the Firm to rely on verification carried out pursuant to points 1-3 of paragraph 5.1.1 above, the verification must have been based at least on a standard level of CDD. It should not be allowed to rely on SDD or any other exceptional form of CDD.

Article 11(3) of the Law

5.1.3. For the purpose of CDD without the Customer being physically present, the Firm must take the required CDD measures as specified in paragraph 2.2. of these Guidelines. This means that the Firm must use additional data, documents or information enabling it to fully perform CDD and ascertaining the authenticity of the Customer's identity.

The information required for the Identification and verification varies per the method that the Firm uses:

Article 11(3) of the Law

5.1.4.

1. In case of methods set in paragraph 5.1.1 parts 1, 4 and 5, the Firm must gather and verify the Identification information set in paragraph 4.2, paragraph 4.8 and paragraph 6.18 of these Guidelines.
2. In case of methods set in paragraph 5.1.1 parts 2 and 3, the Firm must gather and verify the Identification information set in paragraph 4.2 points 1, 2, 3 and 6, paragraph 4.8 points 1-5 and paragraph 6.18 of these Guidelines.

Article 11(4) of the Law

5.1.5. The liability for the compliance with the Customer and BO identification requirements where the Customer is not physically present for the purposes of Identification of the Customer and BO rests with the Firm.

5.2 Third Party Reliance

		General Information
International Legal Standards / Practices	5.2.1.	In certain cases the Customer might have a contact with two or more Firms in respect of the same transaction. E.g. in the retail market the Customer might regularly be introduced by one Firm to another, or deal with one Firm through another; in certain wholesale markets, such as syndicated lending, where several Firms may participate in granting a single loan to a Customer; or a Customer may be an existing Customer of another regulated Firm in the same group.
Article 13 of the Law	5.2.2.	In such cases the Firm has the possibility to use the CDD information gathered by a Third Party. The Firm may obtain the CDD information without the Customer being present by making the use of the Customer or BO-related information obtained from other Financial Institutions and/or Other Obliged Entities or their representative officers abroad, in cases when these Financial Institutions and/or Other Obliged Entities fall within the definition of a "Third Party" defined above.
International Legal Standards / Practices	5.2.3.	A Firm must document the steps taken to confirm that the Third Party relied upon satisfies the definition of the "Third Party" defined above. This is particularly important where the Third Party is situated outside the EU or EEA.
Article 13(2) of the Law	5.2.4.	In case the Firm wishes to use the CDD information on the Customer and BO obtained from the Third Parties, they must have an appropriate agreement in place to ensure that the Third Party will voluntarily perform both of the following conditions: 1. when requested by the Firm, will immediately provide the entire requested information and data regarding the Customer or the BO which must be in possession in accordance with CDD requirements set by law; and 2. when requested, will immediately submit to the requesting Firm the copies of documents related to the Customer or the BO which must be in possession in accordance with the Customer or BO identification requirements set by law.
International Legal Standards / Practices	5.2.5.	A request to forward copies of any identification and verification data and other relevant documents on the identity of the Customer or BO obtained when applying CDD measures, if made, would normally be as part of a Firm's risk-based Customer acceptance procedures. However, the Third Party giving the confirmation must be prepared to provide these data or other relevant documents throughout the period for which it has an obligation under the Law to retain them.
International Legal Standards / Practices	5.2.6.	Where a Firm makes such a request, and it is not met, the Firm will need to take account of that fact in its assessment of the third party in question, and of the ability to rely on the third party in the future, as indicated in paragraph 5.2.7 below.
International Legal Standards / Practices	5.2.7.	Whether a Firm wishes to rely on a Third Party should be part of the Firm's risk-based assessment, which, in addition to confirming the Third Party's regulated status, may include consideration of matters such as: 1. its public disciplinary record, to the extent that this is available; 2. the nature of the Customer, the product/service sought and the sums involved;

3. any adverse experience of the Third Party's general efficiency in business dealings;
4. any other knowledge, whether obtained at the outset of the relationship or subsequently, that the Firm has regarding the standing of the Third Party.

International Legal Standards / Practices 5.2.8. In practice, a Firm relying on the confirmation of a Third Party needs to know:

1. the identity of the Customer and/or BO whose identity is being verified;
2. the level of CDD that has been carried out; and
3. confirmation of the Third Party's understanding of its obligation to make available, on request, copies of the verification data, documents or other information (*inter alia* information on purpose and nature of Business Relationship);
4. the duration for which the Third Party will store the CDD information on a particular Customer. In case the duration is not known (e.g. in case the Third Party has an ongoing Business Relationship with the Customer), the Third Party should inform the Firm about the duration as soon as the information thereof becomes available.

Group Introductions

International Legal Standards / Practices 5.2.9. Where Customers are introduced between different group companies, the Firms that are part of the same group may rely on CDD made by another group company which first dealt with the Customer provided that:

1. the group company being relied upon falls within the definition of the "Third Party"; and
2. the group company being relied upon has carried out the CDD measures pursuant to the requirements of the Law or equivalent EU/EEA Member State or third country requirements.

Article 13(4) of the Law 5.2.10. The Firm is prohibited to use the CDD information related to the Customer and BO obtained from Third Parties if such Third Parties are set up in the high-risk third countries defined by European Commission and the FATF.

International Legal Standards / Practices 5.2.11. There are cases where another group company only introduces the Customer and the Firm and does not give advice, play a part in the transaction between the Customer and the Firm, or have a Business Relationship with the Customer. These cases do not constitute as CDD using the information from Third Parties, and the identification and verification obligations lie with the Firm as the product/service provider.

International Legal Standards / Practices 5.2.12. In cases of intermediaries or agent, or an appointed representative of the Firm, they should be treated as an extension of that Firm. In such a case, the Firm must have in place the appropriate agreement with such an intermediary or an agent, and ensure that such an intermediary or an agent is aware of the appropriate ML/TF requirements and risks associated thereto. This also means that Firm must assure that intermediaries or agent have received necessary AML/CFT trainings to be able to identify potentially suspicious activity and that there is a regular overview of intermediaries or agent's adherence to AML/CFT requirements. Also, even if the intermediary obtains the appropriate CDD evidence, the Firm remains responsible for specifying what should be obtained, and for ensuring that records of the appropriate verification evidence are retained.

International Legal Standards / Practices	5.2.13.	The Firm may also apply the CDD measures by means of an agent or an outsourcing service provider, provided that the arrangements between the Firm and the agent or outsourcing service provider provide for the Firm to remain liable for any failure to apply such measures.
	5.2.14.	An outsourcing service provider should be understood as a person who: 1. performs CDD or a part thereof that would otherwise be undertaken by the Firm, and 2. is not an employee of the Firm.

5.3. Customer and BO Identification and Verification Using Video-Identification Tools

		General Information
Article 11(1)(4) of the Law	5.3.1.	The Firm may establish the identity of the Customer and/or BO where the Customer is not physically present by, among other, using electronic means allowing video-streaming by one of the following methods: 1. the original of the identification document or the equivalent residence permit in Lithuania is captured through video-streaming and the Customer's identity is confirmed by at least the advanced electronic signature in line with the requirements of Article 26 of Regulation (EU) No. 910/2014 (the **First Method**); 2. the Customer's facial image and the original of the identification document or the equivalent residence permit in Lithuania produced by the Customer are captured by way of video-streaming (the **Second Method**).
	5.3.2.	When using the abovementioned video-identification tools for identifying the Customer and the BO, the Firm has to comply with the Technical Requirements.
Technical Requirements	5.3.3.	Customer and/or BO identification can be done by using electronic means allowing video-streaming. The Firm must use special programs, applications or other tools to ensure that the process of taking pictures or making a video is uninterrupted and that it is impossible to transfer images or videos not in real-time. The video-identification tools used also have to record high quality colour video and/ or audio, the records made have to be easy to reproduce and save. It is also important to ensure that the data received by using such tools cannot be altered or used for other purposes incompatible with Customer identification.
	5.3.4.	Customer and/or BO identification using video-identification tools can be performed if at least the following requirements are fulfilled: 1. it is performed in real time; 2. the presented document images and/or the Customer's face must be clearly visible; 3. the continuity of the streaming process is ensured. If the process is discontinued, the identification has to be repeated; 4. the quality of direct video or directly transmitted pictures must be of such quality that allows to easily scan the information from the provided identification documents and to clearly see facial features of the person pictured in the identification document; 5. in case during the video identification the Customer is asked certain questions, the sound recording must be of high quality which ensures that the Customer's answers to questions about their identity can be clearly heard.

	5.3.5.	The Firm must, among other things, store the information and documents confirming the Customer's identity, the identity data of the BO, as well as the video-streaming or a picture transmission data for 8 years from the date of termination of transactions or Business Relationship with the Customer.
	5.3.6.	Further, video recordings and pictures made during Customer and/or BO identification stored by the Firm must contain a mark displaying the following information: 1. name; 2. surname; 3. personal identity number of the Customer; 4. IP address that the Customer used during the identification process (if the Customer used computer equipment for the identification); 5. the date on which the video or picture was taken.
		The First Method
Technical Requirements	5.3.7.	The First Method can be used in two alternative ways: 1. direct video transmission of the identification document: the Customer's original identification document is captured during direct video transmission, and the respective document is displayed in one of the following ways: a) personal identity card and residence permit in Lithuania are displayed from both sides; or b) when demonstrating the passport, displaying the page containing the picture of a natural person and the passport cover. 2. direct transmission of a picture of the identification document: then Customer's original identification document is captured through direct transmission of a picture recording the parts of the document specified in (a)-(b) of point 1 above.
	5.3.8.	After completing the actions indicated above, the Customer has to confirm their identity and the accuracy of provided data by signing the Firm's document for CDD (e.g. questionnaire) using at least an advanced electronic signature complying with the requirements of Regulation (EU) No. 910/2014. Verification by at least an advanced electronic signature must be performed immediately, not later than within 1 hour after completing the actions indicated and must be a part of the same Customer identification procedure.
	5.3.9.	When conducting authentication by an advanced electronic signature, the Firm has to verify the legality and authenticity of the signature.
		The Second Method
Technical Requirements	5.3.10.	Under the second method, the Instruments are used during video-streaming to capture: 1. the Customer's face; and 2. the displayed original identification document.

5.3.11. The Second Method can also be used in two alternative ways:

1. direct video transmission of the Customer's face and of the identification document:
   a) the Customer's face is captured from the front (face and shoulders of the Customer need to be visible, the image must be clearly visible and distinguishable from other objects in the background);
   b) the Customer's frontal facial image and the original identification document must be displayed simultaneously for a certain period of time in order to ascertain the uniformity of Customer's facial features with the facial features of the person pictured in the identification document;
   c) the Customer is asked questions about his identity using an approved Firm's questionnaire;
   d) the pictures of Customer's facial image and the displayed identification document are taken during direct video transmission; or
2. direct transmission of a picture of the Customer's face and of the identification document:
   a) the Customer's facial image is photographed from the front (face and shoulders of the Customer need to be visible, the image must be clearly visible and distinguishable from other objects in the background);
   b) a direct picture transmission of the presented identification document is conducted.

C. IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER

6. Requirements for Identifying the BO and Verifying the BO's Identity

Article 12(1) of the Law 6.1. When performing the CDD, the identity of the BOs must also be established. The identification of the BO means the identification of a natural person or a group of natural persons.

6.2. In general, a BO is an individual who ultimately owns or controls the Customer or on whose behalf a transaction is being conducted. In respect of private individuals, normally, the Customer himself/herself is the BO, unless the Customer itself indicates, or there are features of the transaction, or other circumstances, that indicate otherwise. For the avoidance of doubt, the Firm cannot assume that the private individuals themselves are the BOs of the Customer, and must always first obtain the information from the Customer as to whom the BO is.

International Legal Standards / Practices 6.3. The Firm should be aware that the beneficial ownership information can be obscured through the use of shell companies, complex ownership and control structures involving many layers of shares registered in the name of other legal persons, nominee shareholders and directors, such as close associates and family, and in other ways.

International Legal Standards / Practices	6.4.	In many cases the role of the nominee directors and shareholders is to protect or conceal the identity of the BO and controller of a company or asset. A nominee can help overcome jurisdictional controls on company ownership and circumvent directorship bans imposed by courts and government authorities. Thus, the Firm should be especially aware of the company structures that promote complexity and increase the difficulty to obtain accurate beneficial ownership information. Further, the Firm should be aware of the possibility that there are nominee arrangements in place where friends, family members or associates claim to be the BOs of legal persons, legal arrangements or other undertakings.
	6.5.	Therefore, the Firm must take appropriate and adequate measures to determine the true BOs and identify situations when the beneficial ownership is being obscured.
International Legal Standards / Practices	6.6.	With respect to the public companies listed on a regulated market that are subject to the requirements for the disclosure of the business-related information consistent with EU legislation or subject to equivalent international standards, it should not be understood as the exemption from the requirement to identify their BOs. It does not mean that such companies do not have to identify their BOs, but rather that the regulated market is supposed to have done so already and the information on BOs is available elsewhere.
International Legal Standards / Practices	6.7.	In determining the BO, the Firm must collect data on the Customer's ownership structure and verify it on the basis of documents, data or information obtained from a reliable and independent source. In case of a Multi-Level Ownership the ownership structure scheme must be drafted by or obtained from the Customer.
Article 9(13) of the Law	6.8.	The Firm must also make sure it understands the ownership and control structure of the Customer especially if the ownership and control structure is complex (e.g. the shareholders are from multiple different jurisdictions; the shareholders are of different legal entity / legal arrangement types, there are trusts and private investment vehicles within the ownership and control structure, the Customer has issued bearer shares). The Firm must assess if the ownership and control structure make sense from the commercial, economic or legal perspective.
Article 25(1) of the Law, Article 5.2 of JADIS Regulations	6.9.	The Law requires all companies to maintain information on the BOs and to register the information thereof with the Information System of Legal Entities Participants of the Republic of Lithuania. The registration requirement is not applicable to the public companies listed on a regulated market that are subject to the requirements for the disclosure of the business-related information consistent with EU legislation or subject to equivalent international standards, and legal entities whose sole shareholder is the State or a municipality.
	6.10.	The specific information that has to be provided to the Information System of Legal Entities Participants of the Republic of Lithuania on the BOs is specified in the JADIS Regulations.
	6.11.	The JADIS Regulation may also establish a beneficial ownership calculation method for the purposes of reporting of the BO information to the Information System of Legal Entities Participants.

	6.12.	In practice, for the purpose of CDD, the Firm may use a different beneficial ownership calculation method than the one provided for in the JADIS Regulation.
Article 12(8) of the Law	6.13.	The Firm has the right, when determining the BO, to additionally use the Legal Entity Participant Information System, other state information systems and/or other registers that have information on the BOs. Further, in case the Firm determines discrepancies in the information.
	6.14.	Therefore, in case the Firm uses a different beneficial ownership calculation method, they must have adequate internal procedures in place to determine the BOs pursuant to the method specified in the JADIS Regulations to be able to effectively compare the information on the BOs obtained by the Firm and the one specified in the Legal Entity Participants Information System.
International Legal Standards / Practices	6.15.	Beneficial ownership information of legal persons should be determined as follows: 1. Determining the control through ownership or other means: a) the identity of the natural persons (if any, as ownership interests can be so diversified that there are no natural persons, whether acting alone or together, who exercise control of the legal person through ownership) who ultimately have a controlling ownership interest in a legal person; and b) the identity of the natural persons (if any) exercising control of the legal person through other means. 2. Where no natural person is identified under (a) or (b) above, the Firm should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior manager.
131.3.2 of JADIS Regulations	6.16.	Control through other means may, *inter alia*, include the right to appoint and/or remove the head of the legal entity and/or the members of the management board (or any other collegial management body), the right to approve the annual financial statements relating to the payment of dividends, and/or the right to veto the decisions of the management bodies of a legal person, irrespective of the extent of the ownership (shares or voting rights) it holds.
Article 2(14)(1)(b) of the Law	6.17.	The senior manager of the Customer should be indicated as the BO only in exceptional cases where the Firm puts all reasonable efforts to determine the BO and provided there are no grounds for suspicion that the identity of the BO is being concealed. In this case, the senior manager should be understood as the head (e.g. CEO, managing director, head of administration) of the Customer.
Article 12(2) of the Law	6.18.	When identifying the BO the Firm must request from the Customer the following identity data on the BO: 1. name; 2. surname; 3. personal code. For a foreign national – date of birth (if available – personal code or any other unique sequence of symbols intended for the identification of a person); number of residence permit in Lithuania and its term of validity, place and date of its issuance; 4. citizenship. If the person is stateless – the country which has issued the identification document.

Article 12(5) of the Law	6.19.	The accuracy of the data on the BO has to be confirmed by the Customer's signature and stamp (if the stamp must be held by it according to the legal acts governing its business activities) or by electronic means, or by the Customer's signature on a document in a written form.
Article 12(3) of the Law	6.20.	The Firm has to verify the documents produced by the Customer and the information related to the BO in accordance to the documents, data or information obtained from a reliable and independent source. Such actions have to also involve requesting the Customer itself to indicate the public sources wherein the BO-related information could be verified, such as official registers of legal entities in those countries. This approach is particularly useful in cases where the Customer's ownership structure includes companies incorporated outside the territory of the Republic of Lithuania.
Article 12(6) of the Law	6.21.	The Firm must collect and, if requested by the FIU, submit the following data on the BO: 1. identity data of the BO; 2. proof of verification of the information submitted by the Customer in reliable and independent sources (see section 19 for more information); 3. data on the ownership and control structure of the Customer (legal person).

D. PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP

7. The Requirement to Assess the Purpose and Intended Nature of the Business Relationship

Risk Factors Guidelines	7.1.	The Firm must, *inter alia*, obtain information from the Customer about the intended nature and purpose of the Customer's Business Relationship. Establishing the intended nature and purpose of the Business Relationship is not only a requirement under the laws, but it is also central to understanding the ML/TF risk associated with the Business Relationship and should help the Firm determine what constitutes a suspicious transaction in the context of the individual Business Relationship.
	7.2.	What the Firm does to establish the intended nature and purpose of the Business Relationship can be adjusted on a risk-sensitive basis. E.g. regarding Customers - foreign citizens – the Firm shall take additional measures to establish and verify an intended nature and purpose of Business Relationship to ascertain that there is an apparent economic and lawful purpose.
	7.3.	In all cases the Firm must have sufficient understanding of the intended nature and purpose of the Business Relationship.
	7.4.	The Firm must, where appropriate obtain at least the following additional information about the Customer, e.g.: 1. whether the Customer will use the services of the Firm for their own needs or will represent the interests of another person; 2. contact information; 3. information on the registered address and actual living address of the Customer;

4. information whether the Customer, their Close Family Members, Close Associates or BOs are PEPs;
5. Information on the source of funds related to the Business Relationship or Occasional Transaction referred to in paragraph 1.6;
6. information on the business activities of the Customer (legal person);
7. expected behaviour (e.g. intended transactions, products);
8. purpose of the Business Relationship or Occasional Transactions adhering to the criteria in 1.6. (i.e. why the Customer needs to enter into the Business Relationship or to perform an Occasional Transactions adhering to the criteria in 1.6.);
9. other information.

7.5. In case the Firm determines it necessary, where the Customer is represented by a representative, the Firm may also request the Customer's representative to provide information on the relationship (links) between the Customer and its representative, even in cases where the representative has the necessary authorisations to represent the Customer. It could be relevant for situations where a third person is representing a Customer without the clear business and/or family ties to such a Customer. This information should be taken into account during CDD process.

7.6. In order to ascertain the purpose and intended nature of the Business Relationship, the Firm should also take into account, *inter alia*, whether the Customer (natural person) is a resident or a non-resident. For the purposes of the AML/CFT, a resident (natural person) should be understood as, e.g.:

1. In terms of Lithuanian citizens:
   a) normally, a Lithuanian citizen should be considered as a resident for the purposes of AML/CFT, unless:
      (i) the Customer indicates his/her domicile, registered address and/or actual living address to be outside of Lithuania; and
      (ii) there are other indications that the Customer has permanently left Lithuania, e.g. there are no professional, economic, social or family ties to Lithuania, no financial obligations in Lithuania, etc.

   Such a Customer retains the right to a Basic Payment Account and related daily banking products (such as a payment card and/or Internet bank), however, the Firm should assess whether EDD measures should be applied.

2. In terms of foreign citizens, they should be considered as residents if.:
   a) they indicate their domicile, registered address and/or actual living address in Lithuania; and
   b) they have obtained a temporary or permanent residence permit in Lithuania according to the applicable laws.

If the Customer indicates his/her domicile, registered address and/or actual living address in Lithuania, however, has not yet obtained a temporary or permanent residence permit in Lithuania, the Customer should be considered as a resident of the country which has issued the Customer the personal identification document. In this case, the Firm is required to determine and verify the Customer's economic or family ties to Lithuania in the independent and reliable sources. Absence of prudent evidence of apparent economic or family ties with Lithuania should serve as an indicator that purpose and intended nature of Business Relationship is not sufficiently established.

In such cases the Firm has the right not to establish or continue the Business Relationship or perform Occasional Transaction adhering to the criteria of paragraph 1.6 with such a Customer (and it is strongly recommended to use this right), except as otherwise stated in laws.

The economic and/or family ties to Lithuania could be evident from the following documents and information, e.g.:

1. employment agreement evidencing employment in Lithuania and, if required, a work visa;
2. documents evidencing ownership of entities or other business in Lithuania;
3. other contracts and/or documents evidencing the income of the Customer and/or economic interests of the Customer in Lithuania;
4. documents evidencing the actual living address of the Customer;
5. documents evidencing ownership of immovable property in Lithuania;
6. documents evidencing family ties in Lithuania;
7. other information evidencing economic or family ties to Lithuania.

Article 71(1) of the Law on Payments of the Republic of Lithuania

7.7. In order to ensure financial inclusion, the Firm operating in the territory of an EU/EEA Member State provide an opportunity to open Basic Payment Accounts to Customers who are legal residents in the EU, including persons without a fixed address, asylum seekers, and Customers who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons. However, this possibility only applies to the extent that the relevant Firm can comply with their AML/CFT obligations, i.e. perform CDD.

7.8. Legal persons seeking to use the products and/or services of the Firm must also demonstrate the economic and lawful purpose of the Business Relationship and this information must be assessed by the Firm when assessing the ML/TF risks.

7.9. For the purposes of the AML/CFT, a resident (legal person) should be understood as legal entity registered in Lithuania. Otherwise, such Customers should be treated as residents of a country where they are registered.

7.10. The Firm should take sufficient measures to verify the economic ties to Lithuania of a Customer (legal person) that is not a resident that would explain the purpose of the Business Relationship. In case there are no apparent economic ties that would explain the purpose of the Business Relationship, the Firm may not establish or continue the Business Relationship with such a Customer.

E. CDD CONSIDERATIONS DEPENDING ON A CUSTOMER OR A BUSINESS RELATIONSHIP

8. Financial Institutions and Other Obliged Entities

Financial Institutions

Article 15(1) of the Law	8.1.	If the Firm determines that the situation in relation to the Financial Institution presents a low degree of ML/TF risk, SDD measures may be applied. For more information on SDD measures, please see paragraphs 14.1 – 14.8.

Other Obliged Entities

International Legal Standards / Practices	8.2.	For the purposes of CDD, the Other Obliged Entities should be treated according to the ML/TF risk level and their legal form, e.g. in case of public limited liability companies admitted trading on a regulated market in one or more EU Member States, and other companies from third countries whose securities are traded in regulated markets and which are subject to disclosure requirements consistent with EU legislation, the Law allows the Firm to apply SDD measures if a low ML/TF risk is established, etc.
	8.3.	The Firm should also make sure that the Customer which is an Other Obliged Entity applies a robust and risk-sensitive CDD measures to their own Customers and their Customers' BOs. It may be appropriate for the Firm to take risk-sensitive measures to assess the adequacy of such a Customer's CDD policies and procedures, e.g. by liaising directly with the Customer or by sample-testing the Customer's ability to provide CDD information upon request.

9. Partnerships

Article 6.969 (1) of the Lithuanian Civil Code	9.1.	By means of a partnership (joint activity) agreement, two or more persons (partners) undertake to combine their property, work or knowledge for a certain purpose which is not contrary to the law, or to perform a certain activity.
International Legal Standards / Practices	9.2.	The Firm should also obtain the following data in relation to the partnership: 1. name; 2. business address; 3. names of all partners/principals who exercise control over the management of the partnership; 4. names of individuals who own or control over 25% of its capital or profit, or of its voting rights.
Article 2(14), Article 12(1) of the Law	9.3.	As part of the CDD process, the Firm has to obtain information on all individual BOs owning or controlling more than 25% of the partnership's capital or profit, or its voting rights or who otherwise exercise control over the management of the partnership. The Firm must take reasonable measures to verify the identity of those individuals pursuant to the rules on the identification and verification of BOs.

International Legal Standards / Practices	9.4.	Partnerships and unincorporated businesses, although principally operated by natural persons, or groups of natural persons, are different from Customers (natural persons) due to the fact that there is an underlying business. This business is likely to have a different ML/TF risk profile from that of a Customer (natural person).
International Legal Standards / Practices	9.5.	The Firm shall request to see at least a partnership deed (or other equivalent evidence) to be satisfied that the partnership exists, and check information in an appropriate national register, if available.
	9.6.	The Firm should take appropriate steps to make sure that the person the Firm is dealing with is properly authorised by the Customer.

10. Public Sector Bodies, Governments, Municipal-Owned, State-Owned and Municipal Companies and Supranational Organisations

International Legal Standards / Practices	10.1.	In respect of Customers which are local or foreign governments (or their representatives), supranational organisations, government departments, state-owned companies or local authorities, the approach to identification and verification may be tailored to the circumstances of the Customer, reflecting the Firm's determination of the level of ML/TF risk presented.
Article 15(1)(2) of the Law	10.2.	Where the Firm determines that the Business Relationship presents a low degree of risk of ML/TF and the Customer is a state or municipal authority or institution, SDD measures may be applied.
International Legal Standards / Practices	10.3.	In general, bodies engaged in public administration are different from municipal-owned or state-owned bodies which conduct business. The nature of the Business Relationship established with companies in the financial sector will, therefore, differ. Public administration involves a different revenue/payment stream from that of most businesses, and may be funded from government sources, or from some other form of public revenues. Municipal-owned or state-owned businesses, on the other hand, may engage in a wide range of activities, some of which might involve higher risk factors, leading to a different level of CDD being appropriate. Such entities may be partly publicly funded or may derive some or all of their revenues from trading activities.
International Legal Standards / Practices	10.4.	The Firm should also obtain the following data in relation to the public sector bodies, governments, municipal-owned or state-owned companies and supranational organisations: 1. full name of the entity; 2. nature and status of the entity (e.g., overseas government, treaty organisation); 3. address of the entity; 4. name of the home state authority; 5. names of mangers (or equivalent).

International Legal Standards / Practices	10.5.	The Firm should take appropriate steps to understand the ownership of the Customer, and the nature of its relationship with its home state authority.
International Legal Standards / Practices	10.6.	The Firm should, where appropriate, verify the identities of the managers (or equivalent) who have the authority to give the Firm instructions concerning the use or transfer of funds or assets.
International Legal Standards / Practices	10.7.	Many governmental, supranational, municipal-owned or state-owned organisations will be managed and controlled by individuals who may qualify as PEPs. The Firm needs to be aware of the increased likelihood of the existence of such individuals in the case of such Customers, and, where appropriate, perform EDD having regard to the extent of any risk that the funds of such entities may be used for improper purposes.
International Legal Standards / Practices	10.8.	In case of embassies, the Lithuanian embassies abroad should be considered as Lithuanian residents, whereas embassies of foreign countries in Lithuania should be considered as residents of their country of origin. When determining the BO of the Lithuanian embassy abroad, the Minister of Foreign Affairs of the Republic of Lithuania should be considered as the BO. Similarly, in case of an embassy of a foreign country in Lithuania, usually, a Minister of Foreign Affairs (or equivalent) of that country should be considered as the BO. In case the Customer indicates an ambassador of an embassy of a foreign country in Lithuania as the BO, the Firm may consider an ambassador as BO.

11. Trusts and Foundations

International Legal Standards / Practices	11.1.	There is a wide variety of trusts and foundations, ranging from large, nationally and internationally active organisations subject to a high degree of public interest and quasi-accountability, to small, local trusts or foundations funded by small, individual donations from local communities, serving local needs. The items specified in this section might be helpful for the Firm when dealing with the trust or foundations established in other jurisdictions. It is important, in putting proportionate AML/CFT processes into place, and in carrying out their risk assessments, that the Firm takes account of the different ML/TF risks that foundations of different sizes, areas of activity and nature of business being conducted, present.
Article 2(7), 15(1)(3) of the Law	11.2.	In case the foundation is a collective investment undertaking intended for informed investors, it falls within the category of the Financial Institution as provided for in the Law, and thus, SDD may be performed for such Customer, in case the ML/TF risks are low.
International Legal Standards / Practices	11.3.	For the trusts or foundations that have no legal personality, those trustees (or equivalent) who enter into the Business Relationship with the Firm, in their capacity as trustees of the particular trust or foundation, are the Firm's Customers on whom the Firm must carry out full CDD measures. Following a risk-based approach, in the case of a large, well known and accountable organisation the Firm may limit the trustees considered Customers to those who give instructions to the Firm. Other trustees should be verified as BOs.

International Legal Standards / Practices	11.4.	The identity of the trust or foundation must be verified on the basis of documents or information obtained from a reliable source which is independent of the Customer. This may require to obtain relevant extracts from the trust deed or equivalent foundation agreement, or reference to an appropriate register in the country of establishment.
International Legal Standards / Practices	11.5.	In case of less transparent and more complex structures of trusts or foundations with numerous layers, the Firm should take into account that these entities may pose a higher ML/TF risk. Some trusts or foundations established in jurisdictions with favourable tax regimes may be or might have been in the past been associated with tax evasion and money laundering. In respect of trusts or foundations in this category, the Firm's risk assessment may determine that additional information on the purpose, funding and the BOs of the trust or foundation is obtained.

12. Correspondent Relationships

Article 2(12) of the Law	12.1.	Correspondent relationship means: 1. the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services; 2. the relationships between and among financial institutions, including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.
International Legal Standards / Practices	12.2.	Correspondent institutions are required to perform CDD on the respondent institution, and gather sufficient information about the respondent institution to understand its business, reputation and the quality of its supervision, including whether it has been subject to a ML/TF investigation or regulatory action, and to assess the respondent institution's AML/CFT controls.
Article 14(8) of the Law	12.3.	The Firm is not allowed to commence and proceed with the correspondent relationship or other relationship with a Shell Bank or a bank when it is known that it permits Shell Banks to make use of its accounts. The Firm must take measures enabling to ascertain that the Financial Institutions receiving funds do not permit the use of their accounts to the Shell Banks.
International Legal Standards / Practices	12.4.	The Firm should also take appropriate measures to ensure that the Customer which is a Financial Institution applies robust and risk sensitive CDD measures to their own Customers and their Customers' BOs. It may be appropriate for the Firm to take risk-sensitive measures to assess the adequacy of its Customer's CDD policies and procedures, e.g., by liaising directly with the Customer or by sample-testing the Customer's ability to provide CDD information upon request. In case ML/TF risk is low, the Firm may take SDD measures to perform the identification and verification of a Customer that is a respondent institution. In case the ML/TF risk is high or in case of the performance of the cross-border correspondent relationships with third country Financial Institutions, EDD measures have to be taken.

International Legal Standards / Practices	12.5.	The correspondent institution should also gather sufficient information and determine from publicly available information the reputation of the respondent institution and the quality of its supervision, including whether (and when) it has been subject to a ML/TF investigation or regulatory action.
	12.6.	In addition, the correspondent institution should assess the respondent institution's AML/CFT controls. In practice the Firm may use Wolfsberg Group, Anti-Money Laundering Questionnaire or similar questionnaires developed by the Firm itself to gather such information, or use other methods. Such an assessment should involve reviewing the respondent institution's AML/CFT systems and controls framework. The assessment should include confirming that the respondent institution's AML/CFT controls are subject to independent audit (which could be external or internal). A more detailed/in-depth review should be conducted for higher risk relationships, possibly including reviewing the independent audit, interview of compliance officers, a third party review and potentially an onsite visit.

13. Acquisition of One Financial Services Firm, or a Portfolio of Customers, by another Firm

International Legal Standards / Practices	13.1.	When a Firm acquires the business and customers of another Financial Institution or Other Obliged Entity, either as a whole, or as a portfolio, it is not necessary for the identity of all existing customers to be re-verified, provided that: 1. all underlying customer records are acquired with the business; or 2. warranty is given by the acquired Financial Institution or Other Obliged Entity, or by the vendor where a portfolio of customers or business has been acquired, that the identities of its customers have been verified.
International Legal Standards / Practices	13.2.	Even where the Firm acquires the business and customers from another Financial Institution or Other Obliged Entity, it remains responsible to ensure the compliance with the AML/CFT requirements.
International Legal Standards / Practices	13.3.	It is, however, important that the acquiring Firm's due diligence enquiries include some sample testing in order to confirm that the Customer identification procedures previously followed by the acquired Financial Institution or Other Obliged Entity (or by the vendor, in relation to a portfolio) have been carried out in accordance with Lithuanian requirements.
International Legal Standards / Practices	13.4.	In the event that: 1. the sample testing of the customer identification procedures previously undertaken shows that these have not been carried out to an appropriate standard; or 2. the procedures cannot be checked; or 3. the Customer records are not accessible by the acquiring Firm, verification of identity will need to be undertaken as soon as is practicable for all transferred customers who are not existing verified Customers of the transferee, in line with the acquiring Firm's risk-based approach, and the requirements for existing customers opening new accounts.

F. SIMPLIFIED AND ENHANCED DUE DILIGENCE

14. Application of SDD Measures

Article 15(1) of the Law	14.1.	A Firm may apply SDD measures in relation to a particular Business Relationship or Occasional transaction if both of the following conditions are met: (i) the Firm determines that, taking into account its risk assessment, the Business Relationship or Occasional Transaction presents a low degree of risk of ML/TF; and (ii) it is allowed by Law as indicated in paragraph 14.4.
Risk Factors Guidelines	14.2.	SDD is not an exemption from any of the CDD measures, however, the Firm may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk they identified.
Risk Factors Guidelines	14.3.	The information a Firm obtains when applying SDD measures must enable it to be reasonably satisfied that the risk associated with the Business Relationship is low. It must also be sufficient to give the Firm enough information about the nature of the Business Relationship to identify any suspicious transactions.
Article 15(1) of the Law	14.4.	In case a low ML/TF risk is established, SDD measures can be applied to: 1. companies whose securities are admitted trading on a regulated market in one or more EU/EEA Member States, and other companies from third countries whose securities are traded in regulated markets and which are subject to disclosure requirements consistent with EU legislation; 2. state and municipal authorities and institutions, the Bank of Lithuania; 3. any Customer, if the Customer is a Financial Institution to which the Law applies, or a Financial Institution registered in another EU/EEA Member State or in a third country which has set the requirements equivalent to the requirements of the Law, and monitored by competent authorities for compliance with these requirements; or if international organisations have established a low level of corruption in this country; 4. in cases of life insurance policies or additional voluntary pension accumulation agreements where the annual premium or contribution to the pension fund is no more than EUR 1,000 or the single premium or contribution to the pension fund is no more than EUR 2,500 or an equivalent amount in foreign currency; 5. in cases of insurance policies for pension schemes if there is no clause regarding the early termination before its maturity date, and the policy cannot be used as collateral; 6. in cases of a pension accumulated according to the Law on the Accumulations of Pension of the Republic of Lithuania, also superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

7. electronic money, where a limit of EUR 1,000 or an equivalent amount in foreign currency is imposed on the total amount transacted in a calendar year, except the when an amount of EUR 500 or an equivalent amount in foreign currency, or more is redeemed in that same calendar year upon the electronic money holder's request (applicable to the issuers of electronic money);
8. lotteries, where the monetary value intended for the purchase of lottery tickets and accumulation of amounts of uncollected winnings is kept electronically and the maximum stored monetary value does not exceed EUR 1,000 and is not reloadable or otherwise financed with anonymous funds and cannot be used for other purposes than settlement for the purchased lottery tickets (applicable to companies organising lotteries);
9. cases specified by the ESAs and the European Commission. Please see Annex I for more information;
10. deposits accepted from natural persons, where a limit of EUR 30,000 or an equivalent amount in foreign currency is imposed on the total value of deposits accepted in a calendar year, and the accumulated deposit, interest or other payable amount is returned only to the account held by the Customer in a credit institution from which the funds for the deposit were being transferred, as indicated in point 2 of paragraph 14.5 below.

Article 15(2) of the Law

14.5. When applying SDD measures the Firm may deviate from the requirements to identify the Customer and identify and verify the identity of the BO, but have to take the following actions:

1. obtain the following data:
   a) name, surname and personal code for Customers (natural persons);
   b) name, legal form, registered address, actual business address and legal entity code for Customers (legal persons), and
2. ensure that the first payment of the Customer is performed from the account held in a credit institution, where the credit institution is registered in the EU/EEA Member State or in a third country which has set the requirements equivalent to the requirements of the Law and is monitored by competent authorities for compliance with these requirements.

Article 9(17),(23), Article 15(5), Article 16(1),(2),(3) of the Law

14.6. When applying the SDD measures, the Firm has to comply with the following requirements:

1. perform the ongoing monitoring of the Business Relationship and Occasional Transactions, except in cases of the accumulation of a portion of contributions of the state social insurance pension fund. In case of SDD, the extent of the ongoing monitoring may be adjusted to reflect its determination of the low degree of ML/TF risk;
2. keep the information obtained during the identification and verification of the Customer's identity up to date;
3. report knowledge or suspicion of money ML/TF in case of suspicious monetary operations or transactions.

14.7. It is prohibited to apply or continue to apply SDD measures in the following cases:

1. where the Firm's risk assessment changes and it no longer considers that there is a low degree of risk of ML/TF;
2. in case EDD measures have to be taken;
3. where the Firm suspects ML/TF;
4. where there are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identification or verification.

14.8. In addition to the measures indicated in paragraph 14.5 above, the Firm may also apply one or several additional SDD measures indicated in Annex I of these Guidelines which are consistent with those issued by the ESAs in the Risk Factors Guidelines.

15. Application of EDD Measures

15.1. General Information

Article 14(1) of the Law 15.1.1. In addition to the CDD measures, the Firm must apply EDD measures in cases prescribed by the Law and in any situation which by its nature can present a higher risk of ML/TF. The Firm may establish, under its risk-based approach, that the information it has collected as part of the CDD process is insufficient in relation to the ML/TF risk, and that it must obtain additional information about a particular Customer, the Customer's BO, and the purpose and intended nature of the Business Relationship.

15.1.2. The details on the EDD measures taken and the information obtained during the process of EDD should be duly documented and kept in a manner that would allow to make such information available to the competent authorities if required.

Article 14(1) of the Law 15.1.3. According to the Law, EDD has to be conducted by applying additional Customer and BO identification measures in the following cases:

1. when establishing cross-border correspondent relationships with third country Financial Institutions;
2. when performing Occasional Transactions referred to in paragraph 1.6 or establishing Business Relationships with PEPs;
3. when performing Occasional Transactions referred to in paragraph 1.6 or establishing Business Relationships with the natural persons/legal entities residing/established in the high-risk third countries determined by the European Commission;
4. when performing Occasional Transactions referred to in paragraph 1.6 or establishing Business Relationships with the natural persons/legal entities residing/established in high risk third countries entered on the FATF lists of states that have serious deficiencies in the field of prevention of ML/TF and combating these crimes;
5. if a higher risk of ML/TF is established according to the risk assessment and management procedures set by the Firm.

Article 14(1)(3) of the Law	15.1.4.	With respect to point 3 of paragraph 15.1.3 above, EDD may not be applied with respect to the branches and subsidiaries of Financial Institutions and Other Obliged Entities based in the EU, in which the latter hold the majority interest and which are located in the high-risk third countries determined by the European Commission, provided that: 1. such branches or subsidiaries comply with the requirements of the entire group equivalent to the requirements set by Law; 2. the Firm, after assessing the risks, does not consider that it is necessary to apply EDD measures.
	15.1.5.	In addition to the measures indicated in paragraphs 15.1.3.(2)-(5), the Firm must also apply one or several additional EDD measures indicated in Annex I of these Guidelines which are consistent with those issued by the ESAs in the Risk Factors Guidelines or other additional measures.

15.2. Cross-border Correspondent Relationships with Third Country Financial Institutions

Article 14(2) of the Law	15.2.1.	When conducting the EDD in the case where the cross-border correspondent relationships with third country Financial Institutions are established, the Firm must: 1. gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision; 2. assess AML/CFT controls of the Financial Institutions receiving funds; 3. obtain approval from the Senior Manager before establishing new correspondent relationships. Please see paragraphs 15.7.1-15.7.2 for more information on the Senior Manager. 4. document the respective responsibilities of each of the Financial Institutions; 5. make sure that the respondent institution has properly conducted Customer identification (including verification of the identity of the Customers having direct access to accounts of the correspondent and performance of other identification operations), and that such institution is able to provide relevant Customer identification data to the correspondent institution, upon request.
	15.2.2.	When engaging in correspondent relationships, the Firm must also take appropriate measures applicable to correspondent banks provided for by the ESAs in Risk Factors Guidelines.

15.3. Politically Exposed Persons

International Legal Standards / Practices	15.3.1.	Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher ML risk to the Firm as their position may make them vulnerable to corruption. This risk also extends to their Close Family Members and to the known Close Associates.
	15.3.2.	Where a Customer is a legal person, the Firm should determine whether the manager (e.g. CEO, managing director, head of administration) of the Customer, and the BOs of the Customer are PEPs. In case any of the aforementioned person are PEPs, the Firm must apply the EDD measures applicable to PEPs. In case the Customer is a state or municipal authority or institution, or the Bank of Lithuania, then the Firm may apply SDD measures for such Customers.

	15.3.3.	The Firm should, during onboarding and ongoing due diligence, determine if the Customer is or has become PEP. Such actions should include asking the relevant information from the Customers as well as screening the Customer base against the relevant databases (verifying information in the reliable and independent source). Additionally, the Firm is required at least once a year to screen the Customer base against the relevant PEP databases to determine whether they have not become PEPs, and if an ad-hoc ongoing due diligence is not required.
Article 14(3) of the Law	15.3.4.	In case of Business Relationships or transactions with PEPs, when applying the EDD measures the Firm must: 1. determine and introduce internal procedures which allow determining whether the Customer, its representative, its senior managers (as indicated below) and/or BO are PEPs; 2. receive an approval of the Senior Manager to conclude Business Relationship with such Customers or to continue Business Relationship with the Customers after they become PEPs; 3. take appropriate measures to establish the source of wealth and source of funds related to the Business Relationship or transaction of the Customer and BO who is a PEP; 4. perform enhanced ongoing monitoring of the Business Relationship of PEPs. When determining whether the Customer is a PEP, the Firm must obtain written Customer's declaration on whether the Customer, its representative or the BO is a PEP, and check the relevant reliable and independent databases, e.g. data on private interest declarations could be checked at the Chief Official Ethics Commission of the Republic of Lithuania. It is recommended that such information also include information on the Customer's senior manager (e.g. CEO, managing director, head of administration) (for Customers legal persons).
Article 14(4) of the Law	15.3.5.	Where a PEP is no longer entrusted with a Prominent Public Function, the Firm have to: 1. for at least 12 months take further into account the continuing risk posed by that person; 2. apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to PEPs.

15.4. High Risk Third Countries Determined by the European Commission

Article 14(41) of the Law	15.4.1.	When applying the EDD measures with respect to the natural persons/ legal entities residing/established in high-risk third countries determined by the European Commission the Firm must: 1. obtain additional information on the Customer and BO; 2. obtain additional information about the intended nature of the Business Relationship; 3. obtain information on the source of funds and wealth of the Customer and BO; 4. obtain information on the reasons for the intended or completed transactions; 5. obtain the approval from the Senior Manager to establish Business Relationships with these Customers or consent to continue Business Relationships with such Customers;

6. perform EDD by increasing the number and timing of controls and selecting the types of transactions that will require further investigation;
7. ensure that the first payment by a Customer is made from an account held with a credit institution where that credit institution is established in a EU Member State or in a third country providing equivalent requirements to those of the Law and under the supervision of the competent authorities.

15.4.2. Currently the high risk third countries determined by the European Commission are listed in the Commission Delegated Regulation No. 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies and amended by the following regulations:

1. Commission Delegated Regulation No. 2018/105 of 27 October 2017 amending Delegated Regulation (EU) 2016/1675, as regards adding Ethiopia to the list of high-risk third countries in the table in point I of the Annex;
2. Commission Delegated Regulation No. 2018/212 of 13 December 2017 amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, as regards adding Sri Lanka, Trinidad and Tobago, and Tunisia to the table in point I of the Annex;
3. Commission Delegated Regulation No. 2018/1467 of 27 July 2018 amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, as regards adding Pakistan to the table in point I of the Annex.

Article 14(4²) of the Law

15.4.3. Based on the results of the National Money Laundering and Terrorist Financing Risk Assessment, in case a high level of ML/TF risks in the Republic of Lithuania are identified related to the high risk third countries determined by the European Commission, the Firm, when entering into or conducting international correspondent relationship with financial institutions established in these countries, must take one or several additional measures to effectively reduce the risk of ML/TF:

1. apply additional measures of enhanced Business Relationship monitoring to reduce the risk of ML/TF;
2. make the reporting of suspicious monetary operations and transaction more stringent;
3. limit the Business Relationships or transactions with natural persons or legal entities established in high-risk third countries identified by the European Commission.

If these additional measures are not sufficient to reduce such risk, the Firm should refuse to entire into or cease to conduct, or terminate the international correspondent relationship with such financial institutions.

15.4.4. Since the list of high risk third countries determined by the European Commission is changing, the Firm has to monitor whether the list have not been amended and to take appropriate measures if necessary.

15.5. High Risk Third Countries Entered on the FATF Lists of States That Have Serious Deficiencies in the Field of Prevention of ML/TF and Combating these Crimes

	15.5.1.	Currently the high risk third countries entered on the FATF lists of states that have serious deficiencies in the field of prevention of ML/TF and combating these crime can be found: http://www.fatf-gafi.org/countries/#high-risk. However, since the list is changing, the Firm has to monitor whether the list have not been amended and to take appropriate measures if necessary.
Article 14(5) of the Law	15.5.2.	When applying the EDD measures with respect to the natural persons/ legal entities residing/established in high risk third countries entered on the FATF lists of states that have serious deficiencies in the field of prevention of ML/TF and combating these crimes, the Firm must: 1. receive an approval of the Senior Manager to conclude Business Relationship with such Customers or to continue Business Relationship with such Customers; 2. take appropriate measures to establish the source of wealth and source of funds related to the Business Relationship or transaction; 3. perform enhanced ongoing monitoring of the Business Relationship with such Customers.

15.6. High Risk Customers

Article 14(5) of the Law	15.6.1.	When applying the EDD measures in cases where a higher risk of ML/TF is established according to the risk assessment and management procedures applied by the Firm, they have to take one or several additional Customer and BO CDD measures, at their own discretion (please see Annex I for more information), in order to mitigate the risk, and have to: 1. receive an approval of the Senior Manager to conclude Business Relationship with such Customers or to continue Business Relationship with such Customers; 2. take appropriate measures to establish the source of wealth and source of funds related to the Business Relationship or transaction; 3. perform enhanced ongoing monitoring of the Business Relationship with such Customers.
Based on the Supranational Risks Assessment	15.6.2.	When determining which Customers pose high ML/TF risks, the Firm has to perform a risk assessment on the Business Relationships. Taking into account the outcomes of at least the Firm's Risk Assessment, the National Risk Assessment and the Supranational Risk Assessment, the Firm should take particular care when assessing the ML/TF risks potentially posed by the following persons and entities: 7. traders of goods who, in the course of their business, normally make or receive significant amounts of cash payments; 8. entities operating in the financial subsectors or products that deal with cash (e.g. foreign exchange offices, transfers of funds, certain electronic money products); 9. certain FinTech (i.e. technology-enabled and technology-supported financial services) companies, especially with a high number of non-face-to-face Business Relationships; 10. virtual currency exchange platform operators and/or custodian wallet providers; 11. Other Obliged Entities, especially providers of gabling services and/or lotteries and gaming machines; 12. non-profit organisations; 13. others.

15.6.3. Additionally, when assessing the ML/TF risks potentially posed by the Customers, the Firm should take particular consideration to:

1. the Customers for whom an STR was previously submitted;
2. the Customers who were in the past included in the international or national financial sanctions lists and other;
3. the Customers who are the subjects to a request or information received from the FIU, other pre-trial investigation authorities, the prosecutor's office or a court regarding information about a customer or their monetary operations or transactions that may be related to ML/TF or other criminal activity.

Article 14(10) of the Law

15.6.4. When determining the existence of a higher risk of ML/TF the Firm must assess at least the following factors:

1. characteristics of the Customer:
   a) the Customer's Business Relationship is conducted in unusual circumstances which have no apparent economic or visible lawful purpose;
   b) the Customer's domicile is in a third country;
   c) the legal entities and bodies without legal personality are engaged in the activities of individual property management undertaking;
   d) the company has formal shareholders acting for another person, or holds bearer shares;
   e) cash is dominant in the business;
   f) the equity structure of the legal entity is apparently unusual or excessively complex considering the nature of activities of the legal entity,
2. characteristics of the product, service, transaction or service channel:
   a) private banking;
   b) product or transaction may create favourable conditions for anonymity;
   c) Business Relationship or Occasional Transactions are concluded or performed without physical presence;
   d) payments are received from unknown or unrelated third parties;
   e) product or business practice, including the service provision mechanism, are new, also the use of new or developing technologies involved in the work with both new and former products,
3. characteristics of the territory:
   a) pursuant to the data of reports or similar documents of the FATF or other similar regional organisation, significant non-compliances are established in the system of AML/CFT with the international requirements;
   b) pursuant to the data of governmental and globally recognised non-governmental organisations monitoring and assessing the level of corruption, a high level of corruption or other criminal activity is established in the state;
   c) the state is subject to sanctions, embargo or similar measures imposed, for example, by the EU or the United Nations;
   d) the state finances or supports terrorist activities, or terrorist organisations included in the lists drawn up by international organisations are operating in the territory of the state.

15.7. Other Considerations

Senior Manager Approval

International Legal Standards / Practices

15.7.1. In addition to being aware of the Firm's ML/TF threats, the Senior Manager must have sufficient seniority to make decisions that affect the Firm's risks (e.g. approving appropriate internal policies, control procedures and etc.), and/or otherwise affecting the Firm's ML/TF prevention processes. Depending on the governance structure of the Firm, this should be the employee(s) responsible for the decision making, risk management or similar. Obtaining approval from Senior Manager for establishing, or continuing, a Business Relationship does not necessarily mean obtaining approval from the Board of Directors (or equivalent body), but from a higher level of authority from the person seeking such approval. As risk dictates, the Firm should escalate decisions to more senior management levels.

15.7.2 The appropriate level of seniority for sign off should therefore be determined by the level of increased risk associated with the Business Relationship; and the Senior Manager approving a Business Relationship with a PEP, correspondent relationship with a third country Financial Institution, or another high-risk Customer should have sufficient seniority and oversight to take informed decisions on issues that directly impact the Firm's risk profile. When considering whether to approve such a Business Relationship, senior management should base their decision on the level of ML/TF risk the Firm would be exposed to if it entered into that Business Relationship and how well equipped the Firm is to manage that risk effectively.

Source of Wealth and Source of Funds

15.7.3. When performing EDD, in certain instances the Firm is required to take reasonable measures to establish the source of funds and the source of wealth. It should be noted that the Firm should obtain information on the source of funds of all its Customers for whom CDD measures are applied. When performing EDD, the Firm must take additional steps to verify this information.

15.7.4. The Firm should evaluate each situation individually and request documents that would be useful in the particular situation and would allow to ascertain the legality of the origin of the Customer's funds and wealth.

International Legal Standards / Practices

15.7.5. The "wealth" and "funds" should be understood as two different concepts. The source of wealth refers to the origin of the person's entire body of wealth (i.e., total assets). This information will usually give an indication as to the volume of wealth the Customer would be expected to have, and a picture of how they acquired such wealth. It might be difficult for the Firm to have information about assets of a Customer not deposited or processed by them, however, they may gather such general information from commercial databases or other open sources.

15.7.6. The source of funds refers to the origin of the particular funds or other assets which are the subject of the Business Relationship or Occasional Transaction adhering to the criteria of paragraph 1.6 (e.g., the amounts being invested, deposited, or wired as part of the Business Relationship).

15.7.7. The source of funds or wealth can be verified, by reference to, *inter alia*:

1. an annual tax declaration;
2. an original or certified copy of a recent pay slip;
3. written confirmation of annual salary signed by an employer;
4. an original or certified copy of contract of sale of immovable property and an original extract from a financial institution evidencing the reception of funds obtained from selling the immovable property, if available;
5. an original or certified copy of a will or an equivalent document evidencing the inheritance;
6. an original or certified copy of a donation agreement (either in a simple written form, or certified by a notary public in case notarial form of agreement is required by law);
7. an original or certified copy of a loan agreement (either in a simple written form, or certified by a notary public in case notarial form of agreement is required by law), and extract from a financial institution evidencing the reception or sending of funds related to receiving the loan or receiving the pay-back of a granted loan; or a promissory note (either in a simple written form, or certified by a notary public in case notarial form of agreement is required by law);
8. an internet search of a company registry to confirm the sale of a company;
9. original or a certified copy of the deposit agreement;
10. cash book or cash operations register (for legal persons);
11. other information.

G. MONITORING OF BUSINESS RELATIONSHIPS AND OCCASIONAL TRANSACTIONS, UPDATING AND STORING OF INFORMATION

16. General Requirements for Monitoring

Article 9(16) of the Law

16.1. The Firm must in all cases conduct the ongoing monitoring of the Customer's Business Relationship and Occasional Transactions, including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Firm's knowledge of the Customer, the business and risk profile, and the source of funds.

16.2. All Occasional Transactions have to be also monitored. For the purposes of effective ongoing monitoring of the Occasional Transactions in order to timely determine several related monetary operations or transactions, the Firm has to perform Identification for all Occasional Transactions.

16.3. The personal identification document of the natural person carrying out the transactions should also be checked. Depending on the level of its risk appetite, a Firm might also make copies of such personal identification documents presented by the aforementioned individuals, ask more detailed information from such persons, etc.

17. Updating of Information

Article 9(17); 9(23) of the Law

17.1. In order to ensure that the documents, data or information obtained during the onboarding of the Customer are appropriate and relevant, they must be reviewed and updated by the Firm on an ongoing basis, and at any time when new circumstances emerge or new information appears related to the determination of the risk level of the Customer or BO, their identity details, activities and other relevant circumstances.

17.2. The information on the Customer and BO has to be updated:

1. on an *ad-hoc* basis when new circumstances emerge or new information appears, e.g.:
   a) in case during the ongoing monitoring of a Business Relationship and Occasional Transactions the previously determined ML/TF risk increases; or
   b) in case there are changes in information previously provided by the Customer and BO, e.g. in case the validity of the personal identification document of a Customer expires and the Customer received a new document; the Firm receives new information on the Customer, adverse information in the media, changes in the ownership and/or control structure, changes in the Customer's business model and other. The Firm must duly update the Customer's information in case such information comes to the Firm's attention.

When new circumstances emerge or new information comes to the Firm's attention, the Firm must assess whether it is sufficient to update only that part of the information which to the Firm's knowledge has changed, or if there are any grounds to suspect that the other previously obtained information is also not up to date anymore and should be updated as well. E.g., if the Customer's personal identification document expires it could be sufficient to update only the information on the personal identification document if there are no other grounds to suspect that the other previously obtained information has also changed. However, if the Firm becomes aware that there are changes in the information on the BO, it should be reasonable to update all information on the Customer and the BO obtained during the CDD, in order to make sure that there are no further changes in the Customer's business activity, ownership and control structure, senior management etc.

2. periodically:
   a) in case of low risk Customers for whom SDD was performed: at least once per 3 years;
   b) in case of high risk Customers for whom EDD was performed: at least once per 1 year;
   c) the period for the Customers falling into other risk categories (which are lower than high risk) could be chosen by the Firm based on its risk assessment, however, should occur at least once per 3years.

17.3. In case a document and/or information previously provided by the Customer changes and the Firm can obtain the relevant information from the Population Register of the Republic of Lithuania, there is no need for the Firm to require the Customer to additionally provide such changed document or information.

Article 10(4) of the Law	17.4.	The Firm also may obtain the documents, data or information necessary for the updating of the previously obtained information on the Customer and BO directly from the state information systems or registries, as described in paragraph 4.19.
	17.5.	In non-standard exceptional situations where the Customers may not be reached by the Firm in a standard way (e.g. via Internet banking, during a physical appointment at the Firm), the Firm, pursuant to the risk-based approach, may determine the timing for the update of information and perform this obligation as soon as it is reasonably and practically possible. Such situations may include Customers where a Customer has an established disability or loss of working capacity and cannot visit the Firm and does not use the Internet banking and similar.

18. Implications of the Change in Risk Category

	18.1.	The Firm must periodically review and, in case required, update the Customer's risk assessment in cases where the information and data collected during the Identification and verification of the Customer's identity changes, the Firm obtains new important information on the Customer and its activities, when the Customer requires to use a new product or service, there is a change in the nature of the Customer's activities or operations, monetary operations or transactions are suspicious with respect to ML/TF and other. The Firm must ensure that the risk scoring solutions used by the Firm allow to automatically determine the factors that show an increase in the Customer's risk and to allocate the Customer to an appropriate risk category (as described in paragraphs 3.7-3.15).
Article 9(16) of the Law, Article 19(23) of the Law	18.2.	In case in the course of the ongoing monitoring of the Customer's Business Relationship it is established that the risk of ML/TF previously determined by the Firm has increased, the Firm must take the appropriate CDD or EDD measures (as specified in paragraph 18.5).
Article 14(1) 15(7) (8) of the Law	18.3.	Where the Business Relationship was previously determined as posing a low ML/TF risk and the Customer was identified using SDD measures, the Firm should monitor such a Business Relationship to ensure that the appropriate CDD measures are taken in case during the Business Relationship the risk changes and is no longer low. In case the Customer was identified using CDD measures but the Business Relationship becomes high risk, the Firm has to take appropriate measures and, *inter alia,* perform EDD.
	18.4.	Where the Business Relationship was previously determined as posing a high ML/TF risk and the Customer was identified using EDD measures, the Firm should monitor such a Business Relationship to ensure that the Customer is transferred to another risk category, in case during the Business Relationship the risk changes and is no longer high (e.g. a person ceases to be a PEP).

	18.5.	In case the risk category of the Customer increases during the course of the Business Relationship, the Firm should take the appropriate CDD or EDD measures. If the Firm has previously applied SDD but after the increase of the risk category CDD and/or EDD is required, or if the Firm has previously applied CDD and after the increase of the risk category EDD is required, then these actions should be performed as soon as practically possible, however, no later than within 60 calendar days from the day the Firm has determined that the Customer's risk category has increased. For the avoidance of doubt, the enhanced monitoring of the Business Relationships and transactions should be performed as soon as it is become apparent that the risk level of a Customer has increased; whereas the 60-day term should be applied for such actions as the collection of additional documentation and obtainment of information.

19. Storing of Information

Article 19(10) of the Law	19.1.	The copies of the documents collected on the Customer during the CDD process and during the ongoing due diligence must be stored for 8 years from the date of termination the Business Relationship or Occasional Transaction adhering to the criteria of paragraph 1.6. with the Customer.
Article 19(11) of the Law	19.2.	The correspondence of the Business Relationship with the Customer must be stored for 5 years from the date of Business Relationship or Occasional Transaction adhering to the criteria of paragraph 1.6. with the Customer.
	19.3.	The documents obtained during the CDD and ongoing monitoring process can be stored in a paper form or in electronic form. The Firm must ensure that the relevant data on the Customer, the evidence of the verification of data (e.g. relevant extracts from commercial registers, print-screens, etc.) can be easily obtained in case required by the competent authorities. The relevant information on the Customer, the persons that make up its shareholding structure, the BO and other information should be also stored on the Customer's file on the Firm's systems and should be accessible to the Firm's employees responsible for the Customer.

ANNEX I

This Annex is corresponding to the Joint Guidelines No. JC 2017 37 under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions dated 4 January 2018 issued by the European Supervisory Authorities. As these guidelines might change from time to time, it is recommended for the Firm to update their guidelines on SDD and EDD measures accordingly.

A. Guidelines on SDD Measures

Without prejudice to the requirements set by the Law, SDD measures the Firm may apply include but are not limited to:

3. **Adjusting the timing of CDD**, e.g. where the product or transaction sought has features that limit its use for ML/TF purposes, e.g. by:
   a) verifying the Customer's or BO's identity during the establishment of the Business Relationship; or
   b) verifying the Customer's or BO's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed. The Firm must make sure that:
      (ii) this does not result in a de facto exemption from CDD, that is, the Firm must ensure that the Customer's or BO's identity will ultimately be verified;
      (iii) the threshold or time limit is set at a reasonably low level (although, with regard to terrorist financing, the Firm should note that a low threshold alone may not be enough to reduce risk);
      (iv) they have systems in place to detect when the threshold or time limit has been reached; and
      (v) they do not defer CDD or delay obtaining relevant information about the Customer where applicable legislation, for example Regulation (EU) 2015/847 or provisions in national legislation, require that this information be obtained at the outset.
4. **Adjusting the quantity of information obtained for identification**, verification or monitoring purposes, e.g. by:
   a) verifying identity on the basis of information obtained from one reliable, credible and independent document or data source only; or
   b) assuming the nature and purpose of the Business Relationship because the product is designed for one particular use only.
5. **Adjusting the quality or source of information obtained for identification**, verification or monitoring purposes, e.g. by:
   a) accepting information obtained from the Customer rather than an independent source when verifying the BO's identity (note that this is not permitted in relation to the verification of the Customer's identity); or
   b) where the risk associated with all aspects of the relationship is very low, relying on the source of funds to meet some of the CDD requirements, e.g. where the funds are state benefit payments or where the funds have been transferred from an account in the customer's name at an EEA-Firm.
6. **Adjusting the frequency of CDD updates and reviews** of the Business Relationship, e.g. carrying these out only when trigger events occur such as the Customer looking to take out a new product or service or when a certain transaction threshold is reached; the Firm must make sure that this does not result in a de facto exemption from keeping CDD information up-to-date.
7. **Adjusting the frequency and intensity of transaction monitoring**, e.g. by monitoring transactions above a certain threshold only. Where the Firm chooses to do this, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

The information a Firm obtains when applying SDD measures must enable the Firm to be reasonably satisfied that its assessment that the risk associated with the relationship is low is justified. It must also be sufficient to give the Firm enough information about the nature of the Business Relationship to identify any unusual or suspicious transactions. SDD does not exempt an institution from reporting suspicious transactions to the FIU.

Where there are indications that the risk may not be low, for example where there are grounds to suspect that ML/TF is being attempted or where the Firm has doubts about the veracity of the information obtained, SDD must not be applied. Equally, where specific high-risk scenarios apply and there is an obligation to conduct EDD, SDD must not be applied.

B. Guidelines on EDD Measures

The Firm must apply EDD measures in higher risk situations to manage and mitigate those risks appropriately. EDD measures cannot be substituted for regular CDD measures but must be applied in addition to regular CDD measures.

Politically Exposed Persons

The Firm that have identified that a customer or BO is a PEP must always:

1. Take adequate measures to establish the source of wealth and the source of funds to be used in the Business Relationship in order to allow the Firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity. The measures the Firm should take to establish the PEP's source of wealth and the source of funds will depend on the degree of high risk associated with the Business Relationship. The Firm should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high.
2. Obtain senior management approval for entering into, or continuing, a Business Relationship with a PEP. The appropriate level of seniority for sign-off should be determined by the level of increased risk associated with the business relationship, and the senior manager approving a PEP Business Relationship should have sufficient seniority and oversight to take informed decisions on issues that directly impact the Firm's risk profile.
3. When considering whether to approve a PEP relationship, senior management should base their decision on the level of ML/TF risk the Firm would be exposed to if it entered into that Business Relationship and how well equipped the Firm is to manage that risk effectively.
4. Apply enhanced ongoing monitoring of both transactions and the risk associated with the Business Relationship. The Firm should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring should be determined by the level of high risk associated with the relationship.

Correspondent relationships

The Firm must take specific EDD measures where they have a cross-border correspondent relationship with a respondent who is based in a third country. The Firm must apply all of these measures and should adjust the extent of these measures on a risk-sensitive basis.

The Firm should refer to the Risk Factors Guidelines on EDD in relation to correspondent banking relationships; these guidelines may also be useful for the Firm in other correspondent relationships.

Unusual Transactions

The Firm should put in place adequate policies and procedures to detect unusual transactions or patterns of transactions. Where the Firm detects transactions that are unusual because:

4. they are larger than what the Firm would normally expect based on its knowledge of the Customer, the Business Relationship or the category to which the Customer belongs;
5. they have an unusual or unexpected pattern compared with the Customer's normal activity or the pattern of transactions associated with similar Customers, products or services; or
6. they are very complex compared with other, similar, transactions associated with similar Customer types, products or services,

and the Firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given, it must apply EDD measures.

These EDD measures should be sufficient to help the Firm determine whether these transactions give rise to suspicion and must at least include:

1. taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the Customer's business to ascertain the likelihood of the customer making such transactions; and
2. monitoring the Business Relationship and subsequent transactions more frequently and with greater attention to detail. A Firm may decide to monitor individual transactions where this is commensurate to the risk it has identified.

High risk third countries and other high risk situations

When dealing with natural persons or legal persons established or residing in a high-risk third country identified by the European Commission and in all other high-risk situations, the Firm should take an informed decision about which EDD measures are appropriate for each high-risk situation. The appropriate type of EDD, including the extent of the additional information sought, and of the increased monitoring carried out, will depend on the reason why an Occasional Transaction or a Business Relationship was classified as high risk.

The Firm is not required to apply all the EDD measures listed below in all cases. For example, in certain high-risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the Business Relationship.

EDD measures the Firm should apply may include:

1. **Increasing the quantity of information obtained for CDD purposes**:
   a) Information about the Customer's or BO's identity, or the Customer's ownership and control structure, to be satisfied that the risk associated with the relationship is well understood. This may include obtaining and assessing information about the Customer's or BO's reputation and assessing any negative allegations against the Customer or BO. Examples include:
      (i) information about Close Family Members and Close Associates;
      (ii) information about the Customer's or BO's past and present business activities; and
      (iii) adverse media searches.
   b) Information about the intended nature of the Business Relationship to ascertain that the nature and purpose of the Business Relationship is legitimate and to help the Firm obtain a more complete Customer risk profile. This may include obtaining information on:
      (iv) the number, size and frequency of transactions that are likely to pass through the account, to enable the Firm to spot deviations that might give rise to suspicion (in some cases, requesting evidence may be appropriate);
      (v) why the Customer is looking for a specific product or service, in particular where it is unclear why the Customer's needs cannot be met better in another way, or in a different jurisdiction;
      (vi) the destination of funds and the source of incoming funds;
      (vii) the nature of the Customer's or BO's business, to enable the Firm to better understand the likely nature of the Business Relationship.

2. **Increasing the quality of information obtained for CDD purposes** to confirm the Customer's or BO's identity including by:
   a) requiring the first payment to be carried out through an account verifiably in the Customer's name with a bank subject to CDD standards that are not less robust than those set out in AMLD4;
   b) establishing that the Customer's wealth and the funds that are used in the Business Relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the Firm's knowledge of the Customer and the nature of the Business Relationship. In some cases, where the risk associated with the relationship is particularly high, verifying the source of wealth and the source of funds may be the only adequate risk mitigation tool. The source of funds or wealth can be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent media reports.

3. **Increasing the frequency of reviews** to be satisfied that the Firm continues to be able to manage the risk associated with the individual Business Relationship or conclude that the relationship no longer corresponds to the Firm's risk appetite and to help identify any transactions that require further review, including by:
   a) increasing the frequency of reviews of the Business Relationship to ascertain whether the Customer's risk profile has changed and whether the risk remains manageable;
   b) obtaining the approval of senior management to commence or continue the Business Relationship to ensure that senior management are aware of the risk their Firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;
   c) reviewing the Business Relationship on a more regular basis to ensure any changes to the Customer's risk profile are identified, assessed and, where necessary, acted upon; or
   d) conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that might give rise to suspicion of ML/TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions.

ANNEX II

IMPLEMENTATION PERIODS

Measures related to the proper implementation of the Guidelines on customer due diligence (Guidelines) in order to ensure the uniform application of the customer due diligence requirements among the members of the Association would be mandatory since January 1st, 2021. Paragraph 1.7 would be mandatory after 1 year from the day these Guidelines are approved by the Board of the Association of Lithuanian Banks. We propose these requirements be considered as guidance in the preparatory period.