Rules of procedure and internal audit rules compiled pursuant to Money Laundering and Terrorist Financing Prevention Act

Effective as of February, 2019

These Rules of procedure and internal audit rules are prepared by Trade.io Payment Solutions OÜ, an Estonian private limited company, registered under registry code 14657028, whose legal address is Pärnu mnt 158-88, Tallinn city, Harju county, 11317 (hereinafter the „**Company“**)

The Rules of procedure and internal audit rules consist of:

1) Code of Conduct for the application of customer due diligence measures;

2) Code of Conduct for the collection and preservation of data;

3) Code of Conduct for the performance of the notification obligation and for informing the management;

4) Internal Control Rules.

The rules of procedure:

1) describe transactions of a lower risk level and establish the appropriate requirements and procedure for carrying out such transactions;

2) describe transactions of a higher risk level, including risks arising from telecommunications, information technology means, computer network and other technological development, and establish the appropriate requirements and procedure for carrying out and monitoring such transactions;

3) set out the rules of taking the due diligence measures specified in chapter 3 of the Money Laundering and Terrorist Financing Prevention Act;

4) set out the requirements and procedure for keeping the documents and records specified in the Money Laundering and Terrorist Financing Prevention Act.

The rules of procedure contain instructions for how to effectively and quickly identify whether or not the person is:

1) a politically exposed person;

2) a person whose place of residence or seat is in a country where no sufficient measures for prevention of money laundering and terrorist financing have been taken;

3) a person with regard to whose activities there is prior suspicion that the person may be involved in money laundering or terrorist financing;

4) a person with regard to whom international sanctions are imposed;
5) a person with whom a transaction is carried out using telecommunications.

The rules of procedure are introduced to all employees of an obligated person whose duties include establishment of business relationships or carrying out transactions.

The Company shall regularly check whether the established rules of procedure are up-to-date and establish new rules of procedure where necessary.

Code of Conduct for the application of customer due diligence measures

1. Introduction

1.1. This Code of Conduct for the application of customer due diligence measures is prepared by Trade.io Payment Solutions OÜ, an Estonian private limited company, registered under registry code 14657028 whose legal address is Pärnu mnt 158-88, Tallinn city, Harju county, 11317 (hereinafter the " **Company** ").

1.2. The Code of Conduct for the application of customer due diligence measures is prepared to comply with the Money Laundering and Terrorist Financing Prevention Act and other legal acts of the Republic of Estonia and applicable guidelines.

2. Aim of the Code of Conduct and its elements

2.1. The aim of this Code of Conduct is to ensure the proper identification and verification of customers or persons participating in transactions, as well as ongoing monitoring of business relationships, including transactions carried out during business relationships, regular verification of data used for identification, update of relevant documents, data or information and, when necessary, identification of the source and origin of funds used in transactions.

2.2. Customer due diligence is one of the main tools for ensuring the implementation of legislation aimed at preventing money laundering and terrorist financing and at applying sound business practices.

Customer due diligence comprises a set of activities and practices arising from the organizational and functional structure of the Company and described in internal procedures, which have been approved by the directing bodies of the Company and the implementation of which is subject to control systems established and applied by internal control rules.

2.3. The purpose of customer due diligence is to prevent the use of assets and property obtained in a criminal manner in the economic activities of credit institutions and financial institutions and in the services provided by them whose goal is to prevent the exploitation of the financial system and economic space of the Republic of Estonia for money laundering and terrorist financing. Customer due diligence is aimed, first and foremost, at applying the Know-Your- Customer principle, under which a customer shall be identified and the appropriateness of transactions shall be assessed based on the customer's principal business and prior pattern of payments. In addition, customer due diligence serves to identify unusual circumstances in the operations of a customer or circumstances whereby an employee of the Company has reason to suspect money laundering or terrorist financing.

2.4. Customer due diligence ensures the application of adequate risk management measures in order to ensure constant monitoring of customers and their transactions and the gathering and analysis of relevant information. Upon applying the customer due diligence measures, the Company will follow the principles compatible with its business strategy and, based on prior risk analysis and depending on the nature of the customer's business relationships, apply customer due diligence to a different extent.

2.5. Customer due diligence are applied based on risk sensitive basis, i.e. the nature of the business relationship or transaction and the risks arising therefrom shall be taken into account upon selection and application of the measures. Risk-based customer due diligence calls for the prior weighing of the specific business relationships or transaction risks and, as a result thereof, qualification of the business relationship in order to decide on the nature of the measure to be taken (for instance, normal, enhanced or simplified due diligence measures could be applied).

2.6. If the risk level of a customer or a person participating in a transaction is low, the Company may apply simplified due diligence measures, but is not allowed to skip customer due diligence entirely. If the risk level arising from a customer or a person participating in a transaction is high, enhanced due diligence measures will be applied.

2.7. Upon establishing a business relationship, the Company will identify the person and verify their right of representation based on reliable sources, identify the beneficial owner and, in the case of companies, the control structure, as well as identify the nature and purpose of possible transactions, including, if necessary, the source and origin of the funds involved in the transactions.

2.8. Customer due diligence measures are appropriate and with suitable scope if they make it possible to identify transactions aimed at money laundering and terrorist financing and identify suspicious and unusual transactions as well as transactions that do not have a reasonable financial purpose or if they at least contribute to the attainment of these goals.

2.9. The first requirement for the measures of prevention of money laundering and terrorist financing is that the Company does not enter into transactions or establish relationships with anonymous or unidentified persons. Legislation requires that the Company waives a transaction or the establishment of a business relationship if a person fails to provide sufficient information to identify the person or about the purpose of the transactions or if the operations of the person involve a higher risk of money laundering or terrorist financing. Also, legislation requires the Company to terminate a continuing contract without the advance notification term if the person fails to submit sufficient information for application of customer due diligence measures.

2.10. The Company ensures that information concerning a customer (incl. gathered documents and details) is up to date. In the event of customers or business relationships falling in the high risk category, the existing information will be verified more frequently than in the event of other customers/business relationships. The respective data shall be preserved in writing or in a form that can be reproduced in writing and made available to all relevant employees who need it to perform their employment duties (management board members, account managers, risk managers and internal auditors).

2.11. The principles and instructions provided for in the customer due diligence measures are set out in the internal procedures of the Company. Independent control mechanisms are established over adherence to these procedures and the relevant training of employees are ensured.

3. Applicability of the Code of Conduct

3.1. This Code of Conduct for the application of customer due diligence measures includes:

3.1.1. requirements for the identification and verification as well as methods for the collection of relevant data, including requirements for the data and documents on which the identification is based;

3.1.2. procedures for the identification of the purpose and intended nature of business relationships and transactions prior to the conclusion of such transactions or long-term contracts, and procedures for ongoing monitoring of business relationships;

3.1.3. a description of low risk transactions and requirements for and procedures of the conclusion of such transactions;

3.1.4. a description of high risk transactions and requirements for and procedures of the conclusion and ongoing monitoring of such transactions;

3.1.5. procedures for updating the data and documents used for identification and verification;

3.1.6. other issues arising from the aim and scope of the Code of Conduct.

4. General Obligatory Identification Rules

4.1. The Code of Conduct for the application of customer due diligence measures requires the identification and verification in case of:

4.1.1. establishing business relationships with persons with whom the Company has no previous business relationships;

4.1.2. conducting transactions with persons with whom the relationship between the person and the Company will not constitute a business relationships and whereby the amount transferred exceeds EUR 15 000, or an equal amount in any other currencies, whether in one-time transfer or several related payments over a period of up to one year;

4.1.3. establishing business relationships with persons in respect of whom simplified due diligence measures are applied;

4.1.4. establishing business relationships with politically exposed persons;

4.1.5. conducting transactions through means of communication with persons with whom the Company has a business relationship;

4.1.6. establishing business relationships with persons whose place of residence or registered office is in a country where the application of measures for the prevention of money laundering and terrorist financing is insufficient.

5. Organization structure

5.1. The management board of the Company shall regularly (not less than once a quarter) review the efficiency of the internal procedures implemented for the purpose of complying with the Money Laundering and Terrorist Financing Prevention Act and ensure internal control over following the internal procedures. The Company shall appoint the person(s) who is (are) responsible at the management board level for the application of the customer due diligence measures provided for in the Money Laundering and Terrorist Financing Prevention Act. The competence and responsibilities of the person shall transparently and unambiguously arise from internal documentation regulating the tasks and functions of the members of the management board (e.g. rules of procedure of the management board, job descriptions of the members of the management board and service contracts of the members of the management board).

5.2. The person(s) appointed by the management board of the Company shall ensure the application of customer due diligence measures based on the provisions in legislation and other so-called Rules of Procedure and take into account that the measures applied are adequate, correspond to the operating profile of the service provider and comply with the customer, nature and scope of the transactions and the related risks of money laundering or terrorist financing.

5.3. The management board of the Company ensures that the resources allocated to comply with the Money Laundering and Terrorist Financing Prevention Act are sufficient and that the employees directly involved in the fulfilment of the requirements of the Money Laundering and Terrorist Financing Prevention Act are fully aware of the requirements of the Money Laundering and Terrorist Financing Prevention Act.

5.4. Each executive and employee directly involved in the implementation of the Money Laundering and Terrorist Financing Prevention Act shall have professional skills that allow them to fully and with sufficient accuracy adhere to the provisions of legislation in accordance with the scope of their responsibilities and they shall have completed the respective training or been otherwise instructed therein by the Company.

5.5. The Company shall mitigate and prevent conflicts of interests with internal rules, whereby the grounds of remuneration of executives and employees encourage them to disregard or deviate from provisions of law.

5.6. Customer due diligence is part of the overall risk management framework where a clear distinction shall be made between the application of customer due diligence measures applied in business relationships and the application of measures for prevention of money laundering and terrorist financing in the Company's own operations.

5.7. The Company shall provide contractual partners (in the event of outsourcing) and all relevant staff, including staff whose duties include the establishment of business relationships and/or the execution of transactions, management of customer relationships, with regular training in and notification about the nature of the risks of money laundering and terrorist financing and any new trends in the field. First and foremost, staff shall be kept informed about the requirements governing the prevention of money laundering and terrorist financing with respect to the application of customer due diligence measures and reporting on suspected money laundering.

5.8. The Company shall ensure that the customer due diligence measures and data collection and preservation requirements applied in its third-country representations, branches or majority held subsidiaries comply with the Money Laundering and Terrorist Financing Prevention Act and the requirements set out in other act and guidelines. In a situation where it is not possible to fulfil such requirements due to the specific nature of local laws, the Estonian Financial Supervision Authority will be notified thereof immediately.

6. Economic or professional activities via agents and outsourcing

6.1. the Company has the right, taking account the special requirements and restrictions provided by law, to use the services of a third party under a contract the subject of which is the continuing performance of activities and continued taking of steps required for the provision of (a) service(s) by the Company to its customers and that would normally be performed and taken by the Company itself. For the purposes of this section, third parties include, for instance, agents, subcontractors and other persons to whom the Company transfers the activities relating to the provision of the services provided as a rule by the Company in its economic activities.

6.2. The Company shall choose the third party in order to ensure the ability of the person to fulfil the requirements provided for in the Money Laundering and Terrorist Financing Prevention Act and to ensure the reliability and the required qualifications of such a person.

6.3. The third party specified in section 6.1 is subject to all of the requirements provided by law for prevention of money laundering and terrorist financing regarding outsourced activities. The Company who outsourced its activities is liable for infringement of the requirements.

6.4. Upon outsourcing an activity (activities), the Company shall ensure that the third party has the knowledge and skills required, above all, for the identification of situations of a suspicious and unusual nature and is able to meet all of the requirements for the prevention of money laundering and terrorist financing provided by law. To comply with the provisions in this section, the Company shall ensure the notification of the executives of the third party of the relevant requirements and the training of its staff in the prevention of money laundering and terrorist financing.

6.5. Upon outsourcing an activity to third parties, the Company shall ensure that any documents and information collected for the fulfilment of requirements arising from legislation are preserved in accordance with the procedure established in the Money Laundering and Terrorist Financing Prevention Act and any legislation issued on the basis thereof. The contract shall ensure that relevant information is handed over to the Company and that the relevant information and documents are archived in accordance with its rules of procedure.

6.6. The outsourcing contract shall specify the rights and duties of the Company upon reviewing compliance by the third party with the requirements provided by law. The outsourcing of economic activities to a third party shall not impede state supervision over the Company and the latter shall, under contract, grant competent authorities access to the third party for supervisory purposes to whom the Company has outsourced its duties, tasks or functions.

6.7. Whilst services are provided by third parties, situations where the application of customer due diligence measures to the required extent is possible to an insufficient degree or entirely impossible shall be avoided. A third party shall be able to fully apply the required customer due diligence measures, thereby being able to notify the contact person of the Company immediately and to decline a transaction. The Company shall, under contract, ensure its right to terminate the contract with the third party if the latter fails to perform its contractual duties or obligations or performs the unduly.

6.8. The Company shall immediately notify the Financial Supervision Authority of entry into a contract serving as the basis for outsourcing its activity (activities).

7. Appointment of a compliance officer

7.1. Thee management board of the Company shall appoint amongst management board members a compliance officer. The functions of a compliance officer may be performed by one employee or member of the management board or several employees and/or a structural unit with the relevant duties. If the

functions of the compliance officer are performed by a structural unit, the head of the relevant structural unit will be responsible for the performance of the functions.

7.2. The position of a compliance officer within the organizational structure of the Company shall allow for the performance of the requirements provided by law for the prevention of money laundering and terrorist financing. Upon establishment of the compliance officer position, the compliance officer shall be made directly accountable to the management board of the Company and made as independent of business processes as possible.

7.3. The compliance officer's independence from business processes does not mean that the officer is prohibited to advise or train colleagues for the purpose of ensuring the compliance of the actions of the executives and employees with the requirements of the Money Laundering and Terrorist Financing Prevention Act.

7.4. The professional qualifications and skills of the compliance officer shall meet the requirements established in the Money Laundering and Terrorist Financing Prevention Act and the compliance officer's professional and business reputation shall be impeccable.

7.5. The functions of the compliance officer are as follows:
7.5.1. organization of collection and analysis of information referring to unusual transactions or transactions suspected of money laundering or terrorist financing in the activities of the Company (collection of information means collection of any and all suspicious or unusual notices received from the employees, contractual partners and agents of the Company, and systemizing and analysis of the information contained in them);

7.5.2. reporting to the Financial Intelligence Unit (hereinafter the FIU) in the event of suspicion of money laundering or terrorist financing (notice being given in the manner agreed with the FIU);

7.5.3. periodic submission of written statements on implementation of the rules of procedure to the management board of the Company; and

7.5.4. performance of other obligations related to the fulfilment of the requirements of the Money Laundering and Terrorist Financing Prevention Act by the credit institution or financial institution (including instructing and training employees and applying respective control mechanisms).

7.6. The compliance officer shall have access to the information forming the basis or prerequisite for establishing a business relationship, including any information, data or documents reflecting the identity and business activity of the customer. The management board also grants the compliance officer the right

to participate in the meetings of the management board if the compliance officer deems this necessary to perform their functions.

7.7. The contact details of the compliance officer shall be communicated to the Financial Supervision Authority. The compliance officer shall inform the Financial Supervision Authority within a reasonable term about the appointment of a new compliance officer or a change in contact details.

8. Risk-based approach

8.1. The Company shall recognize, assess and understand money laundering and terrorist financing risks in its own activities and in the activities of its customers and take measures to mitigate the risks. The applicable measures shall correspond to the identified risk level.

8.2. In the event of the risk-based approach, the Company shall assess the probability of the realization of risks and what the consequences of their realization are. Upon assessment of probability, the chance of an increase in the threat and the possibility of occurrence of the respective circumstances shall be taken into account, e.g. the possible threats that may influence the activities of the customer and the service provider shall be taken into account.

8.3. The Company shall take all customer due diligence measures. The scope of taking the measures depends on the characteristics of the given business relationship or the risk level of the person or customer participating in the transaction or official act; thereby the Know-Your Customer principle shall be followed. The Money Laundering and Terrorist Financing Prevention Act provides for a few exceptions to the automatic application of certain customer due diligence measures, e.g. the amount-based reporting obligation in accordance with subsection 3 of § 49 of the Money Laundering and Terrorist Financing Prevention Act.

8.4. Upon identifying and substantiating the risk levels of a customer or a person participating in a transaction, the Company shall take into account, among other things, the following risk categories:

8.4.1. Customer risk whose factors arise from the person or customer participating in a transaction; among other things, the following shall be taken into account:

8.4.1.1. the legal form, management structure, field of activity of the person, including whether it is a trust fund, civil law partnership or another similar contractual legal entity or a legal person with bearer shares;

8.4.1.2. whether it is a politically exposed person;

8.4.1.3. whether the person is represented by a legal person;

8.4.1.4. whether a third party (individual) is the beneficial owner;

8.4.1.5. whether the identification of the beneficial owner is impeded by complex and non-transparent ownership relations;

8.4.1.6. the residency of the person, including whether it is a person registered in a territories with a low tax rate;

8.4.1.7. whether the person is subject to an international sanction;

8.4.1.8. the possibility of classifying the customer as a typical customer of a certain customer category;

8.4.1.9. circumstances (including suspicious transactions identified in the course of a prior business relationship) resulting from the experience of communicating with the person, its business partners, owners, representatives and any other such persons;

8.4.1.10. the duration of the operations and the nature of business relationships;

8.4.1.11. the type and characteristics of the service provided or product sold (whether the service or product is unusual or economically impracticable);

8.4.1.12. whether the service or product may be related to crime or development of weapons of mass destruction;

8.4.1.13. whether the person participates in transactions where cash plays a major role (e.g. currency exchange locations and gambling operators);

8.4.1.14. whether the person's customers are the same or change constantly;

8.4.1.15. whether the person's customer base has increased rapidly;

8.4.1.16. whether the person renders the service to anonymous customers;

8.4.1.17. the existence and nature of the risk factor relating to a service provider used to forward the service or product;

8.4.1.18. the type and characteristics of the services used or products consumed by the person outside the Company;

8.4.1.19. the nature of the personal activities of an individual;

8.4.1.20. whether the origin of the person's assets or the source and origin of the funds used for a transaction can be easily identified; and

8.4.1.21. whether the person has been identified face-to-face or via the Internet.

8.4.2. Product or service risk, whose risk factors result from the customer's economic activities or the exposure of a specific product or service to potential money laundering risks, among other things:

8.4.2.1. private banking and personal banking;

8.4.2.2. currency exchange and conversion transactions;

8.4.2.3. provision of alternative means of payment and e-money;

8.4.2.4. purchase and sale of high-value goods;

8.4.2.5. provision of online advertising;

8.4.2.6. provision of innovative services; and

8.4.2.7. foundation, sale and administration of companies.

8.4.3. Country or geographical risk, whose factors arise from differences in the legal environment of various countries:

8.4.3.1. whether the country applies legal provisions that are in compliance with the international standards of prevention of money laundering and terrorist financing;

8.4.3.2. whether there is a high crime rate (incl. drug-related crime rate) in the country;

8.4.3.3. whether the country cooperates with a criminal group; whether criminal groups use the country to pursue their operations;

8.4.3.4. whether the country engages in proliferation;

8.4.3.5. whether there is high level of corruption in the country;

8.4.3.6. whether international sanctions have been or are being imposed on the country; and

8.4.3.7. whether other measures have been taken against or positions of international organizations have been expressed on the country.

8.5. Taking account of the aforementioned risk categories, the Company shall determine the risk level of the person or customer participating in a transaction, e.g. whether the customer's money laundering or terrorist financing risk level is low, normal or high or whether it corresponds to other risk level qualifications determined and used by the Company.

8.6. To determine the impact of each risk category, the Company shall assess the likelihood of occurrence of risk factors in the risk category. To determine the impact of a specific risk category, the qualifying quantity of occurrence of the risk factors characterizing it may be used for the purpose of deeming a specific risk factor as „having an impact" or as „not having an impact" in the event of exceeding a certain threshold.

8.7. Certain guidelines in the event of specifying a low level of risk.

8.7.1. The customer's risk level is generally considered low if there is no risk factor of impact in any risk category and it can therefore be claimed that the customer and its operations demonstrate elements that do not differ from those of an ordinary and transparent person; thereby there is no reason to suspect that the customer's operations may increase the probability of money laundering and terrorist financing.

8.7.2. In a situation where the application of the required measures of customer due diligence arises from legislation and information about the customer and its beneficial owner is publicly available, where the operations and transactions of the person are in line with its day-to-day economic activities and do not differ from the payment conventions and conduct of other similar customers or where the transaction is subject to quantitative or other absolute restrictions, the Company may deem the customer's estimated money laundering or terrorist financing risk to be lower.

8.7.3. In a situation where at least one risk category can be qualified as high, the risk level of money laundering or terrorist financing cannot usually be low. Equally, a low risk does not necessarily mean that the customer's operations cannot be associated with money laundering or terrorist financing at all.

8.7.4. If the risk resulting from a business relationship, a customer or transaction is low due to risk factors established with respect to the party to the transaction or the customer and the other conditions set out in § 32 of the Money Laundering and Terrorist Financing Prevention Act have been fulfilled, the Company may apply simplified due diligence measures, but may not omit the customer due diligence measures entirely. Upon application of customer due diligence measures by way of the simplified procedure, the Company may determine the scope of application of the customer due diligence measures.

8.8. Certain guidelines in the event of specifying a high level of risk

8.8.1. The customer's risk level is usually high, when assessing the risk categories on the whole it seems that the customer's operations are not ordinary or transparent; there are risk factors of impact due to which it may be presumed that the likelihood of money laundering or terrorist financing is high or considerably higher. The customer's risk level is also high if a risk factor as such calls for this. A high risk does not necessarily mean that the customer is laundering money or financing terrorists.

8.8.2. If the Company feels that the risk level of a customer or a person participating in a transaction is high, the Company shall apply customer due diligence measures pursuant to the enhanced procedure in order to adequately manage the respective risks. Thereby enhanced due diligence measures shall be applied in accordance with § 37 of the Money Laundering and Terrorist Financing Prevention Act.

8.9. Specific risks related to virtual currency trade and means of risk mitigation

8.9.1. The AML/CFT risks specific to virtual currency trade are:

8.9.1.1. the anonymity provided by the trade in virtual currencies on the internet;

8.9.1.2. the limited identification and verification of participants;

8.9.1.3. the lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for these transactions that are segmented across several countries;

8.9.1.4. the lack of a central oversight body.

8.9.2. The Company and its employees shall apply the following means to mitigate the above specific risks:

8.9.2.1. the transactions of virtual currency trade and exchange shall be made using the customer's bank account;

8.9.2.2. the Company shall not engage in any transactions where a party to the transaction remains anonymous or the party cannot be sufficiently identified according to the present rules;

8.9.2.3. upon each transaction whereby the value of the transaction exceeds 15 000 euros or an equal sum in another currency the Company shall require from customers evidence of the source of the virtual currency used by the customer in the transaction.

8.10. The Company shall document the determination of the risk level, update it and make the data available to competent authorities, if necessary.

9. Establishment of business relationships

9.1. The terms of a long-term contract underlying a business relationship shall also be included in the general terms and conditions of the provision of services by the Company and/or in the general and/or other standard terms and conditions of a settlement contract or other contracts.

9.2. The Company shall identify each customer upon establishment of a business relationship and upon making a transaction if the value of the transactions of the customer per year exceeds.

9.3. The business relationships between Company and customers are regulated by contracts made in writing, in a form that can be reproduced in writing or electronically.

9.4. The prerequisite for the establishment of a business relationship is an explicit and recorded certification by the customer that it will fulfil the conditions established by the Company for the establishment of the business relationship and execution of transactions.

9.5. The internal procedures of the Company shall set out the terms and conditions on the basis of which the services to be used by the customer and the scope of the services will be determined. The Company shall make certain in advance that the services provided match the substance of the actual declarations of intent by the customer, are in accordance with the nature and purposes of the given contract and correspond to the risk level attributed to the customer.

9.6. The rules of procedure regulating the establishment of a business relationship shall, in addition to provisions of law, contain the following:

9.6.1. the procedure for introducing the prerequisites for the establishment of a business relationship, entry into long- term contracts and execution of transactions (including the procedure for recording the customer's declaration of intent and identification of the purpose of the business relationship and the transaction) by the Company;

9.6.2. the requirement for receiving confirmation from the customer that the customer is aware of and has understood the duties and obligations established by the relevant conditions, including the request for information required for the establishment of the business relationship by and the form of submission of the information.

9.7. Upon the establishment of a business relationship, the customer or its representative and the representative of the Company shall be in the same place. This means that a potential customer or its representative has a direct contact with the representative of the Company. A direct contact calls for direct communication between the representative of the Company and the customer for the purpose of assessing the compliance of the substance of the customer's declaration of intent and purpose with the customer's true will. Thereby it is possible to specify the customer's risk level more accurately with the help of what is experienced in the course of the direct contact. The contact may occur outside the principal place of business of the Company if, in the course thereof, at least the same customer due diligence measures are performed as in ordinary instances.

9.8. In events provided by law the Company a business relationship may be established without a direct contact (i.e. without being in the same place as the customer), provided such procedure is formulated in the rules of procedure of the Company.

9.9. The instances and procedure for the establishment of business relationships without direct contact shall be provided in respective procedural rules, including measures for subsequent customer due diligence measures and the management of related risks. The rules of procedure for the establishment of a business relationship without direct contact shall set out a procedure by applying which it is possible to ensure compliance with the conditions set out in the Money Laundering and Terrorist Financing Prevention Act. The rules of procedure shall set out at least the following:

9.9.1. a code of conduct for accepting or executing payment instructions prior to the application of all the customer due diligence measures;

9.9.2. a code of conduct in a situation where identification of the person and other information is performed using electronic means of identification;

9.9.3. the code of conduct for a situation where the required customer due diligence measures cannot be applied (a person cannot be identified within the prescribed time limit), as a result of which the customer's declarations of intent cannot be accepted;

9.9.4. a code of conduct in a situation where it is ensured that, in the event of the digital identification of an individual, international payments cannot be made in excess of and transaction-related and service-related sums do not exceed the limit of 15 000 euros per year; and

9.9.5. a code of conduct for terminating a business relationship established without direct contact.

9.10. Upon the establishment of a business relationship without direct contract, the following can be used upon verifying data submitted to identify a person:

9.10.1. a notarized or certified copy of an identity document submitted in writing or electronically;

9.10.2. electronic methods of identification, thereby verifying the validity of the electronic signature and certificate; and

9.10.3. data collected by the Company and/or public databases for the purpose of verifying the personal identification code, registry code and data of the representatives of the company and the address. The Company may use other legible documents to identify a person, including certification by other credit institutions, notaries, foreign missions, public authorities and foreign business partners.

9.11. For entry into a long-term contract with the Company, an appropriate attitude of the parties is presumed, as a result of which the Company shall set out constraints in their rules of procedure with the aim of avoiding unnecessary risks and ensuring the establishment of respective relationships at a suitable time and in a suitable place. In the event of business relationships established without direct contact, not only risks relating to a single transaction, but to all similar transactions and the service as a whole and their impact at the institutional level shall be taken into account.

9.12. The purpose of application of customer due diligence measures is not merely the identification of the customer. Sufficient application of customer due diligence measures means a situation where, among other things, the customer's risk level is determined.

9.13. In the event of extraordinary termination of a business relationship on grounds resulting from § 42 of the Money Laundering and Terrorist Financing Prevention Act, different time limits for provision of services (above all, restrictions on making transactions) and termination of a business relationship (long-term contract) may be established. In the event of extraordinary termination of a business relationship, the internal procedures of the

Company shall set out a procedure for the subsequent use of the customer's assets (e.g. allowing for a payment to be made to the account of a credit institution in another contracting state of the European Economic Area or in an equivalent third country). No disbursements in cash are allowed.

10. Customer Due diligence measures

10.1. Customer due diligence measures shall also be applied in the event of suspicion of money laundering or terrorist financing or if the Company has doubts about the correctness of the documents or other data submitted by a customer, i.e. when circumstances differing from ordinary behavior and referring to the existence of risk factors of impact become evident in a customer's actions. Customer due diligence measures shall also be applied in a situation where it is reasonable to presume that it may constitute money laundering or terrorist financing or where the Company is not convinced of the sufficiency of the applied measures. The list of customer due diligence measures set out in the Money Laundering and Terrorist Financing Prevention Act contains the minimum criteria and is imperative. The
Company shall also take other customer due diligence measures that have not been provided by law, given the customer's field or region of activity as well as the characteristics of the transaction and related risks.

10.2. The Company shall, in addition to the customer due diligence measures provided by law, comprehensively evaluate the substance and purpose of the customer's transactions and actions, relying on the universally recognized professional skills characteristic of credit institutions and financial institutions to identify a possible link between a transaction, step or funds and money laundering or terrorist financing.

10.3. The Company has sufficiently applied the customer due diligence measures for the purposes of subsection 1 of § 20 of the Money Laundering and Terrorist Financing Prevention Act if it is convinced that it has sufficiently applied the obligation arising from the aforementioned provision. The principle of reasonableness is taken into account upon assessing conviction.

11. Customer identification

11.1. The Know-Your-Customer (KYP) principle shall be followed upon customer identification. This principle means that the operating profile, purpose of operation, beneficial owner of the person as a potential customer and, if necessary, the source and origin of the funds used in the transactions and other similar information essential for the establishment of a business relationship shall be identified in addition to the person. Upon making transactions, the customer shall be identified and the compliance of transactions shall be assessed based on the customer's main fields of activity and prior payment behavior.

11.2. In line with the risk-based approach, the Company shall choose, among other things, the suitable scope of the KYC principle.

11.3. The Company shall identify the customer and the beneficial owner within a reasonable period of time prior to the commencement of the steps for entry into a long-term contract or while entering into the contract. A person participating in the transaction shall be identified prior to the commencement of the steps for entry into the long-term contract or while entering into the contract.

11.4. Any information and documents concerning establishment of identity shall be preserved in a manner making it possible to respond fully and without unreasonable delay to relevant enquiries from the FIU, investigating body, court or supervision authority. To this end, the Company shall set up a system enabling, in view of the characteristics of its activities, the prompt retrieval from databases and documents of the required information or document concerning identification of the customer or person participating in the transaction.

11.5. Identification and verification of persons upon the establishment of a business relationship are mandatory in the event of the use of any and all financial services, regardless of whether a long-term contract is entered into with the person participating in the transaction or not, thereby taking into account the exceptions arising from the Money Laundering and Terrorist Financing Prevention Act.

12. General requirements regarding identification of individual upon establishment of business relationship

12.1. The establishment and verification of the identity of an individual (a natural person) shall be carried out, as a general rule, in one step on the basis of an identity document. The address, operating profile, profession and field of activity, purpose and characteristics of establishment of a business relationship, beneficial owner (if necessary) and other similar information essential for the establishment of a business relationship shall be identified in addition to identifying the person.

12.2. An individual shall be identified based on an identity document in accordance with § 21 of the Money Laundering and Terrorist Financing Prevention Act. A document submitted to the Company for identification shall be assessed as follows:

12.2.1. validity of the document based on the date of expiry;

12.2.2. the outward likeness and age of the person match the appearance of the person represented on the document;

12.2.3. the personal identification code matches the gender and age of the submitter; and

12.2.4. with respect to information contained in codes assigned to individuals of a foreign country, foreign missions or other competent authorities shall be consulted in the case of doubt as to the authenticity of the document or identity.

12.3. A copy of the page containing personal data and a photo shall be made of the identity document in accordance with 21 of the Money Laundering and Terrorist Financing Prevention Act. The copy made of the document shall be of a quality allowing the details included on it to be read legibly. Any details specified by law shall be recorded.

12.4. The Company shall register the occupation and address of the individual in the course of identification and verification of identity on the basis of the person's statements and a utility bill provided by the person. As for the place of residence, not the address recorded in the population register or another similar register but the permanent or primary place of residence of the person is important. If it is difficult to determine a person's permanent place of residence (e.g. the person's place of residence cannot be identified or there are several of them), the person's habitual residence shall be identified. A post office box number or poste restante address cannot be considered a habitual residence.

12.5. Upon identifying the permanent place of residence or habitual residence of an individual, it is also necessary to register the address of the place to which the Company can send notices on paper.

12.6. In addition to the address of the place of residence of the individual, the Company may record other contact details, including an e-mail address, phone number, Facebook account, Skype account and other similar data, and agree on the submission of information via these telecommunications channels.

12.7. Determining field of activity, job or profession gives the Company the opportunity to assess whether the business relationship or transactions are in compliance with the customer's normal participation in

commerce and whether the business relationship or transaction has a clear economic reason. For the purpose of prevention of the movement of illegally acquired funds, the customer's operating profile needs to be identified upon establishment of a business relationship. To this end, the customer's main fields of work and activity and possible payment habits need to be identified. It is important to pay attention to persons with whom the customer enters into transactions and to their seat.

12.8. Upon identifying an individual, it shall be identified whether the person is a politically exposed person.

12.9. Any details and references required to identify a person shall be verified by means of reliable and independent sources of information (e.g. national registers, authorities, credit institutions, foreign missions of the Republic of Estonia and foreign missions in the Republic of Estonia or based on documents and other information certified by other relevant authorities). In exceptional instances (if the use of reliable and independent sources of information is impossible), copies of documents or information communicated by unofficial representatives or mediators or other dependable information (incl. handwritten statements by a person) may be relied on to identify a person. The Company shall, prior to entering into transactions or taking steps with the person to be identified, make certain that the information obtained in such a manner is sufficient. In such an instance, a notation to this effect shall be made on the copies confirming identification, and thereafter the legality of the details and documents shall be verified immediately.

12.10. The identification or recommendation of a person by the executives, other customers or business partners of the Company may contribute to the identification of the customer, but the respective recommendations do not substitute for the identification requirements contained in the Money Laundering and Terrorist Financing Prevention Actor release the Company from the fulfilment of the requirements.

12.11. Even if the Company knows the customer personally or the customer is a public figure, the internal identification procedure provided by law cannot be disregarded. The identity of the public figures and persons directly or indirectly related to them who address the Company for performance of transactions or taking of steps shall be verified.

12.12. In the event of persons whose active legal capacity is limited (incl. minors), the Company shall also follow the identification procedure. Upon identification of the personal data of minors, the Company shall, in addition to the instructions given in these Guidelines and provisions of the Money Laundering and Terrorist Financing Prevention Act, follow the provisions of the General Part of the Civil Code Act and the Family Act. In addition to the personal data of a person of restricted active legal capacity, the personal data of the legal representative (parent(s) or guardian(s)) shall be verified.

12.13. The Company shall regularly update the customer's personal data and operating profile, ensuring that they are up to date and based on the customer's risk level.

13. Politically exposed persons

13.1. The Company shall establish internal procedures in order to decide whether a potential customer or its beneficial owner is a politically exposed person of a contracting state of the European Economic Area or third country, a domestic politically exposed person or a person who is or has been entrusted with a prominent function by an international organizations.

13.1.1. The Company shall identify the close associates and family members of politically exposed persons only if their link to a person carrying out significant duties of public authority is known to the public or if the Company has reason to believe that such a link exists.

13.1.2. With regard to politically exposed persons, Company shall take the following measures in addition to relevant customer due diligence measures:

13.1.2.1. request the required information from the customer, incl. take immediate measures to identify the sources of wealth and funds used in the framework of the business relationship or transaction;

13.1.2.2. collect data or make an enquiry with the respective databases or public databases;

13.1.2.3. make an enquiry or verify information on the webpages of the relevant supervision authorities or institutions in the country of location of the customer or person.

13.2. The establishment of a business relationship with a politically exposed person shall be decided by the management board of the politically exposed person or the person(s) authorized by the management board. If a business relationship with a customer has been established and the customer or the beneficial owner later proves to be or becomes a politically exposed person, the management board (or persons authorized by the management board) shall be informed.

13.3. The Company shall exercise regular enhanced supervision in business relationships established with a politically exposed person (except in cases provided by law).

13.4. Regular supervision shall also be exercised by the Company after a politically exposed person has ceased to be a politically exposed person if the Company feels, based on the risk-based approach, that the person still entails a higher risk.

14. Identification of beneficial owner of individual

14.1. Upon identifying an individual, the Company shall, in the event of doubt, also identify the beneficial owner of the individual, i.e. the person who controls the actions of the individual.

14.2. A doubt about the existence of a beneficial owner may arise, above all, if the Company perceives, upon applying customer due diligence measures, that the individual has been swayed to establish the business relationship or enter into the transaction. In such an event the person who exercises control over the individual shall be deemed the individual's beneficial owner.

14.3. It shall be taken into account that the scope of customer due diligence, including upon identifying the beneficial owner, is related to the risk of money laundering and terrorist financing, which depends on the type of customer, its country of origin, business relationship, product, service or transaction.

15. Civil law partnerships and other contractual associations

15.1. Upon identification of civil law partnerships, all of the members of the partnership or their representatives shall be identified on the grounds applicable to individuals. The beneficial owners of the partnership shall be identified.

15.2. In the case of civil law partnerships, the purpose of their activity and, if necessary, the origin of the funds used shall be identified. Thereby one may rely, among other things, on clarifications and statements given by the representative of the partnership. The Company shall make sure that the use of funds by the partnership corresponds to the purposes of activity declared by it previously.

15.3. Data of the members of the partnership and their representatives shall be preserved and regularly updated.

16. General requirements regarding identification of legal entity upon establishment of business relationship

16.1. The business name, registry code, seat and place of business, information about the legal form, passive legal capacity, representatives (legal representatives and those authorized to represent the legal entity before the Company) and beneficial owners shall be identified upon identifying legal entities. The operating profile, business partners, purpose of operation, purpose of establishment and characteristics of business relationships and other similar information required for the establishment of business relationships shall be identified as well.

16.2. Upon determining the seat of a legal entity, both the theory of the country of foundation as well as the theory of the seat shall be used to identify whether the legal entity may involve country and geographical risks.

16.3. The place of business of a legal entity shall be determined on the basis of factual circumstances, i.e. where production is based or a service is provided.

16.4. The identification and verification of the identity and passive legal capacity of a legal entity shall be carried out, as a general rule, on the basis of the information contained in the commercial register (in Estonia) or another equivalent register or a copy of the registration certificate or an equivalent document (for instance, in countries where there is no national register, foundation documents certified by a notary are considered equivalent) submitted in accordance with the procedure provided by law. Documents issued by a register or their equivalents shall have been issued no earlier than 6 months prior to their submission to the Company.

16.5. Documents issued in a foreign state shall be legalized or apostilled, i.e. in order to use an official document issued in one country in another, an internationally recognized certificate of the authenticity of the document is given in another.

16.5.1. Documents issued by Lithuanian, Latvian, Polish, Ukrainian or Russian authorities and officials do not require legalization or an apostille.

16.5.2. To be legalized, a document shall go through the legalization authorities of the issuing state as well as those of the receiving state (usually, foreign ministries).

16.6. Upon identification, legal entities are not required to submit an extract of their registry card if the Company has access to the required extent via the computer network to the data in the commercial register or register of non-profit organizations and foundations (including access to data in respective registers in the foreign country).

16.7. Upon identification of a legal entity, the Company is required to register the names of the executive of the legal person or members of its management board or another body substituting for it, their powers in representing the legal entity and the principal field of activity of the legal entity. If the aforesaid details are not indicated by the register extract or another relevant document, the relevant information shall be obtained by using other documents and/or reliable sources of information.

16.8. The need for use, the criteria of use and/or the list of reliable sources of information shall be specified by the Company (e.g. information issued by national registers, public authorities, credit institutions, foreign missions of the Republic of Estonia and foreign missions in Estonia may be used).

16.9. The Company shall identify the existence of politically exposed persons related to the legal entity. If no respective links appear in the information about a politically exposed person obtained from the representative of the legal entity, an enquiry shall be made with the respective databases in the event of suspicion.

16.10. In the case of international organizations, the documents serving as the basis for their activities (including in Estonia) shall be determined and the submission of relevant documents shall be requested. If necessary, information required for the establishment of the business relationship which is contained in the documents shall be verified.

17. Agency

17.1. The Company shall verify if the person is acting on their own behalf or on behalf of another (natural or legal) person. If the person is acting on behalf of another person, the Company shall also identify the person on behalf of whom transactions are performed.

17.2. Documents required to identify a legal entity shall be submitted by the legal representative or authorized representative of the entity. The Company shall make certain that the right of representation complies with legislation. If the submitted documents do not indicate the right of representation of the individual submitting them and/or the authority is not compliant, the identification process (and thus also the establishment of the business relationship or performance of the transaction) cannot be continued.

17.3. The Company shall identify the basis, scope and term of the representative's right of representation. The representative shall be asked to submit a document proving the right of representation. Further attention shall be paid to the verification of the identity and right of representation of authorized representatives operating or residing in a jurisdiction different from the legal entity's jurisdiction or whose rights of representation are valid for more than a year.

17.4. Clarification shall be sought on the scope of the right of representation granted to the authorized representative (for instance, whether a one-off transaction or recurring transactions over a certain period are involved). The Company shall take notice of the terms of the right of representation granted to the authorized representative and provide services only to the extent of the right of representation.

17.5. Under subsection 5 of § 22 of the Money Laundering and Terrorist Financing Prevention Act, the Company has the right to request that the representative of a legal entity of a foreign country submit documents proving their right of representation, notarized or certified in an equivalent manner and legalized or certified with an apostille, unless provided for otherwise in an international agreement.

17.6. Upon handling the right of representation of authorized and legal representatives, it shall be made certain whether the representative knows their customer. To identify the true nature of the relationships between the representative and the represented, the representative shall know the substance and purpose of the declarations of intent by the represented party and be able to answer other relevant questions about the seat of operations, fields of activity, sales and transaction partners, other related persons and beneficial owners. In addition, the representative shall confirm with their signature that they are aware and convinced of the source and legal origin of the funds used in the transaction of the represented entity.

18. Identification of beneficial owner

18.1. Upon the identification of a legal entity, the Company shall register the beneficial owner of the entity.

18.2. In a situation where no person holds or identifiably controls more than 25%, the circle of beneficial owners will be identified pursuant to the principle of proportionality, according to which information shall be requested about the shareholders, partners and other persons who exercise control or other significant influence over the activities of the legal entity.

18.3. If the identification documents of a legal entity or other submitted documents do not indicate the beneficial owner of the entity, the relevant information (including information about membership of the group of companies and the ownership and management structure of the group of companies) shall be registered on the basis of the statements or a handwritten document of the representative of the entity.

18.4. In order to verify information identified on the basis of statements or a handwritten document, reasonable measures shall be applied (e.g. the filing of a query with relevant registers) and the submission of the annual report or another relevant document of the legal entity shall be requested.

18.5. The Company may use a risk-based approach and take sufficient measures to verify the identity of the beneficial owner with the aim of making certain as to whom the beneficial owner in the business relationship or transaction is. With respect to compliance with this requirement, the Company is left with several options in order to decide:

18.5.1. the extent to which public information about shareholders or members will be used;

18.5.2. the extent to which relevant information will be requested orally or to record obtained information in writing or in a form that can be reproduced in writing;

18.5.3. in which cases the customer will be asked to complete a respective questionnaire; or

18.5.4. what other options can be used and are practicable in the event of the Company.

18.6. It shall be taken into account that the scope of customer due diligence with respect to the customer (incl. identification of the beneficial owner) is related to the risk of money laundering and terrorist financing, which depends on the type of customer, their country of origin, business relationship, product, service and transaction.

18.7. Higher attention shall be paid to companies founded in territories with a low tax rate, whose beneficial owners are often difficult to identify.

18.8. The Company can consider a person who exercises control in another manner, without having a 25% shareholding in the company, as the beneficial owner. This situation arises when the Company suspects that a third party whose links to a company cannot be legally proven or are difficult to prove the exercises of control over management of a legal person.

19. Requirements for identification of non-resident legal entities

19.1. In the event of the identification of legal entities that are non-residents, the Company shall comply, to the greatest extent possible, with the same requirements as in the event of customers that are residents, taking into account the specifications arising from the country of origin and legal form of the non-resident customer. Due to differences in legal regulations in different countries, the rules of procedure of the Company shall also set out detailed requirements and guidelines for the identification of the passive legal capacity of the legal entity by means of other documents and/or reliable information sources.

19.2. Upon identifying the passive legal capacity of a non-resident legal entity and handling documents certifying the powers of representatives, it shall be verified whether the documents meet the requirements established in Estonian legislation with respect to legalization of foreign documents.

19.3. Due to differences in legal regulation in different countries, the Company shall pay attention, above all, to companies founded in countries or territories with a low tax rate, because it is not always abundantly clear whether they have passive legal capacity. In many countries, the standards for identifying a customer

and registration and preservation of documents are lower than in Estonia, as a result of which particular attention shall be paid to the content of the documents of the companies registered in such countries and to the manner of their submission.

19.4. Particular attention shall be paid to information and documents submitted in the case of persons whose country of origin is on the FATF's list of countries that do not contribute sufficiently to the prevention of money laundering. The Company shall avoid business relations with persons whose place of residence or location is in the country listed by FATF high risk and non-cooperative countries. That list can be seen at: http://www.fatf-gafi.org/countries/#high- risk .

19.5. In the event of foreign-language documents, the Company is entitled to request a translation of the documents into a language understood by it. The use of translations should be avoided in a situation where the original documents have been prepared in a language understood by the Company (e.g. the translation of English-language original documents into Russian).

20. General requirements regarding the application of customer due diligence measures upon execution of transactions

20.1. In addition to the establishment of a business relationship, customer due diligence measures shall also be taken if:

20.1.1. in the event of any kind of transaction, incl. in the event of an offer made in the course of provision of a counselling service whose price exceeds the limit specified in the Money Laundering and Terrorist Financing Prevention Act. Thereby it is irrelevant whether the pecuniary obligation is performed by means of cash or cashless settlements;

20.1.2. the amount of a single transaction or the total amount of consecutive transactions exceeds the limit provided by law (or the internal procedure rules of the Company). The obligation shall be performed upon occasional transactions made by a non-customer;

20.1.3. the Company has doubts about the correctness or sufficiency of the data collected upon establishment of the business relationship and if the actions of the other party are not ordinary or transparent as well as if the Company suspects money laundering or terrorist financing; and

20.1.4. the Company does not suspect money laundering or terrorist financing for the purposes of subsection 1 of § 49 of the Money Laundering and Terrorist Financing Prevention Act and does not have the reporting obligation for the purposes of subsection 3 of § 49 of the Money Laundering and Terrorist

Financing Prevention Act, but the transaction is complex and extraordinarily large or the transaction scheme is unusual and does not have an obvious economic or legal purpose.

20.2. The Company shall constantly assess changes in the customer's operations and whether these may raise the risk level so that additional customer due diligence measures need to be taken.

20.3. The application of customer due diligence measures also calls for the existence of the respective monitoring systems whose purpose is to detect reaching the transaction limit or the existence of risk factors and inform the appropriate persons thereof for the purpose of identifying suspicious or unusual transactions. If the Company comes to suspect money laundering in the course of monitoring transactions, the FIU shall be informed thereof.

21. Following transactions

21.1. The following of unusual and suspicious transactions is an important part of the set of customer due diligence measures applied by financial institutions and allows for the identification of circumstances that may point to money laundering or terrorist financing in the economic activities of customers. Also, the purpose of following a customer's transactions is to identify transactions with subjects of international sanctions and politically exposed persons and detect and notify of transactions whose limit or other parameters exceed the prescribed value over a certain period of time.

21.2. Transaction-following measures can be divided into two. One can use measures which enable, based on parameters or features developed with the help of the Company’s prior work experience, transactions to be followed in real time as well as analyzed afterwards.

21.3. Screening

21.3.1. In the event of following transactions in real time, customer executives or other employees observe, upon performing their duties, the customer's behavior and transactions with the aim of detecting unusual or suspicious transactions or transactions exceeding the prescribed limits.

21.3.2. Upon following transactions in real time, information technology tools which, using predefined parameters, select transactions made over a certain period shall be used. The screening parameters depend on information technology possibilities and established goals. What shall be identified is as follows:

21.3.2.1. politically exposed persons involved in transactions;

21.3.2.2. transactions with persons whose name, date of birth etc. match data disclosed in lists of persons subject to international sanctions;

21.3.2.3. transactions with persons whose country of operation or origin is included on the list of higher (terrorist) risk countries; and persons whose transactions are subject to one-off temporary monitoring.

21.4. Monitoring

21.4.1. Upon monitoring transactions, measures shall be taken to verify the submission of information required about the payer upon money transfer. In order to help detect suspicious transactions, payment service providers should take measures to detect the absence of payer-related information in payment instructions.

21.4.2. With the help of monitoring systems, the recipient's payment service provider shall check whether the reporting or payment and settlement system fields used for making the transaction have been filled with the symbols or input used in the reporting or payment and settlement system with regard to the information relating to the payer.

21.4.3. Using monitoring systems, payments with insufficient data about the payer (incl. the payer's name, address and account number) shall be identified among the payments of the payment service provider of the payer. Thereby the payer's address can be replaced with the payer's date and place of birth, customer number or personal identification code, and if the payer does not have an account number, the payment service provider of the payer will replace it with a unique feature with the help of which the payer can be identified.

21.4.4. For the purpose of analyzing transactions afterwards (monitoring), one can analyze transactions separated from the mass of transactions based on predefined parameters. Transactions it is not possible to interfere with during execution (e.g. transactions made via an ATM) are the main objects of monitoring. In addition, upon subsequent monitoring of transactions, the largest transactions based on the sum, currency and customer type over a certain period are analyzed. A list of typical parameters on the basis of which transactions can be selected for monitoring is given below:

21.4.4.1. single large international payments (e.g. whereby the sum ends with at least four zeros);

21.4.4.2. international payments whose description contains the words „loan", „deposit", „payback" etc.;

21.4.4.3. accounts (of individuals and legal entities) with the highest turnover in the period under review based on currencies (of individuals and legal entities);

21.4.4.4. the largest transactions (of individuals and legal entities) in the period under review (of individuals and legal entities) based on different currencies;

21.4.4.5. transactions made via an ATM which exceed a certain limit over the period under review;

21.4.4.6. cash withdrawals in a bank branch based on currencies as well as individuals and legal entities which exceed a certain limit;

21.4.4.7. single transactions that exceed the limit, which are made by customers whose turnover is small;

21.4.4.8. sudden upsurge in turnover of holders of correspondent banks‟ VOSTRO accounts;

21.4.4.9. transactions with persons whose country of operation or origin is on the list of higher (terrorist) risk countries;

21.4.4.10. payments to high-risk countries;

21.4.4.11. payments relating to risky banks; and

21.4.4.12. transactions of specific customers or customer types.

21.5. If the payment service provider of the recipient notes that the required information about the payer is missing or incomplete upon receiving a payment, the recipient shall refuse the transaction or request full information about the payer.

21.6. If the customer is regularly unable to give the requested information about the payer, the Company shall take measures which include giving warnings and setting time limits. Thereafter the recipient may refuse to enter into any transactions with the customer or limit or terminate the business relationships with the customer. The payment service provider of the recipient informs the FIU thereof.

22. Conduct in case of suspicion of money laundering and fulfilment of reporting obligation

22.1. In a situation where the Company, based on documents collected in the course of application of customer due diligence measures, develops a suspicion of money laundering or terrorist financing upon the

establishment of a business relationship or upon occasional making of transactions, the Company shall not establish the business relationship or make the occasional transaction.

22.2. If unusual circumstances or circumstances whereby an employee of the Company suspects money laundering or terrorist financing become evident in relationships with a customer, the compliance officer appointed by the executive/management board shall be immediately informed thereof and the compliance officer will decide the immediate forwarding of the information to the FIU and the need to postpone or refuse to make the transaction. In a situation that entails a high risk of money laundering or terrorist financing, an employee of the Company may decide to postpone the transaction and thereafter inform the compliance officer of the situation.

22.2.1. The background of each individual suspect or unusual instance shall be investigated as much as reasonably necessary, thereby recording the details of the transaction and analyzing the circumstances with the aim of identifying the typical features of more frequent transactions.

22.2.2. The main circumstances to which attention should be paid when suspect and unusual transactions are analyzed are as follows:

22.2.2.1. What is suspicious about the steps, transactions or other circumstances?

22.2.2.2. Is the Company convinced that it knows its customer sufficiently or is it necessary to collect additional information about the customer?

22.2.2.3. Upon taking a step or making a transaction involving identifying a customer or the customer's representative, the Company shall make certain that it follows the prescribed procedure. Was all the required information submitted or did additional information need to be requested or otherwise clarified?

22.2.2.4. Have there been repeated instances of suspicious steps and transactions?

22.3. If the postponement of a transaction could cause significant losses to the parties, its omission is impossible or may prevent the interception of the potential perpetrator of money laundering or terrorist financing, the transaction or official act shall be performed and thereafter a report shall be forwarded to the FIU.

22.4. The rules of procedure of the Company shall set out a code of conduct for the staff of the Company regarding the postponement of a transaction or official act.

22.5. The rules of procedure of the Company shall set out both the conditions for the forwarding of information to the FIU as well as for the preservation of the forwarded information.

22.6. The Company shall preserve in a form that can be reproduced in writing all of the information received from staff about suspicious or unusual transactions and any information collected to analyze these reports and other related documents and any reports forwarded to the FIU along with information about the time of the forwarding of the report and the employee that forwarded it.

22.7. No customer or party participating in a transaction (including its representative or other related parties) with respect to whom suspicion is being communicated to the FIU may be notified of this.

22.8. The Company shall immediately fulfil the reporting obligation. The purpose of immediate fulfilment is to give the FIU the chance to develop the suspicion specified in subsection 1 of § 57 of the Money Laundering and Terrorist Financing Prevention Act and for taking its own measures. Money laundering is a process where criminal proceeds, above all, financial assets may be transferred via credit institutions and financial institutions of multiple states in a single day and therefore swift reporting helps to track down illegal funds more effectively.

23. Correspondent relationships

23.1. In order to establish a correspondent relationship with a credit institution or financial institution of a third country, the Company shall obtain consent from the management board and, for the purpose of application of enhanced due diligence measures: collect sufficient information about the correspondent institutions in order to fully understand the nature and reputation of the business operations of the institution; also obtain certification as to the quality of exercising supervision over it. Any possible connection of the correspondent institution with a suspicion of money laundering or terrorist financing, relevant investigation steps or sanctions shall be checked in public sources; evaluate the institution's mechanisms for the prevention of money laundering and terrorist financing and make certain that these are adequate and effective; and document the obligation/responsibility of both parties to the correspondent relationship in the field of the prevention of money laundering and terrorist financing, including the exchange of relevant information (entry into a relevant contract).

23.2. The contract for a correspondent relationship entered into with a credit and financial institution from a third country or the rules of procedure of the relevant Company shall set out the obligations of the parties, including the conditions for the application of customer due diligence measures to payable-through accounts, i.e. correspondent accounts to which a third party has direct access to effect transactions in its name, with respect to customers with access.

23.3. The Company is not allowed to open a correspondent account in a so-called shell bank or a bank where a shell bank has accounts. Correspondent accounts shall not be opened in a bank where evaluation of the reliability of executives and of measures to prevent money laundering and terrorist financing uncovers deficiencies in view of relevant international standards or the circumstances serving as the basis for evaluation.

23.4. The Company shall not establish a correspondent relationship with an institution or company in any other third country that is not a credit institution or financial institution under Estonian law, yet whose principal and sustained business activity is similar to banking.

24. Foreign affiliates and subsidiaries

24.1. The Company registered in Estonia applies customer due diligence measures and the requirements for information collection and preservation that are at least equivalent to the provisions of the Money Laundering and Terrorist Financing Prevention Act in all foreign offices, branches and majority-held subsidiaries of the companies of the consolidation group, if such affiliates and subsidiaries are founded.

24.2. If the legislation of the third country does not permit the application of equivalent measures, the Company shall apply supplementary measures to prevent money laundering or terrorist financing.

24.3. The Company operating in several different countries, including in a third country, shall avoid in their activity the application of standards differing by country. Standards approved in the European Union provide guidance.

25. Changes to the Code of Conduct

25.1. The Company shall from time to time review these rules in order to comply with the applicable law.

ANNEX 1: Risk assessment model in accordance with clause 9 of the Code of Conduct for the application of customer due diligence measures

This Annex sets out the risk assessment model for the application of customer due diligence measures.

Four categories associated with the person participating in the transaction shall be taken into account upon risk assessment:

I. place of residence or seat of the person participating in the transaction – country and geographical risks shall be taken into account;

II. parameters characterizing the person participating in the transaction – customer risk shall be taken into account;

III. economic activities of the person participating in the transaction – product and service risks shall be taken into account; and

IV. transaction partners of the person participating in the transaction and risks related to them – the customer risk of the transaction partners of the person participating in the transaction, the country and geographical risks and the product and service risks shall be taken into account.

Upon assessment of these risks, each risk category shall be assessed on a scale of 3 points where:

The risk is low	There are no risk factors of impact in any risk category and the customer and the customer's operations are transparent and do not deviate from the operations of an average, reasonable person engaged in the same field. Thereby there is no suspicion that the risk factors on the whole might cause the realization of the threat of money laundering or terrorist financing.
The risk is medium	There is one risk factor or there are several risk factors in the risk category, which differ(s) from the operations of a person engaged in the same field, but the operations are still transparent. Thereby there is no suspicion that the risk factors could, on the whole, cause realization of the threat of money laundering or terrorist financing.
The risk is high	There is one feature or there are several features in the risk category which, on the whole, undermine the transparency of the person and the person's operations, as a result of which the person differs from a person operating in the same field. Thereby the realization of the threat of money laundering or terrorist financing is at least possible

Next, the score should be totaled, attributing the coefficient of 2 to category 4. Thereafter the total amount should be divided by 4. The average of the categories determines whether the risk category of the person participating in the transaction is high, medium or low. Example: The seat of the person participating in the transaction is Estonia. It is a domestically operating company engaged in providing construction services to Estonian customers.

Risk Level Risk Category	Low Score – 1	Medium Score – 2	High Score – 3	Coefficient	Impact on risk level
1. Place of residence or seat of person participating in transaction	1			1	1
2. Parameters characterizing person participating in transaction	1			1	1
3. Economic activities of person participating in transaction	1			1	1
4. Transaction partners or person participating in transaction and persons related to them	1			2	2
Average	N/A	N/A	N/A	N/A	1,25

If the average of the categories is under 2, it should be noted that the customer cannot have a low risk category if at least one of the categories has a high risk. The customer's overall risk category is also high if a risk factor as such calls for this.

Parameters of determining customer's risk

level the customer's risk level is low – x < 2

the customer's risk level is medium – 2 ≤ x ≤

2.75 the customer's risk level is high – x >

2.75

ANNEX 2: Criteria of low risk of money laundering and terrorist financing which allows the application of simplified customer due diligence measures

(1) This Annex shall be applied to obligated persons within the meaning of Article 2 (1) of the Money Laundering and Terrorist Financing Prevention Act.

(2) The Company may refer to this Annex in cases specified in Division 3 of Chapter 3 of the Money Laundering and Terrorist Financing Prevention Act.

(3) This Annex shall not be applied if it appears from publicly available information that the risk of money laundering or terrorist financing related to a client or a transaction is not low.

General requirements for the application of simplified customer due diligence measures

(1) The Company may apply simplified customer due diligence measures describing low risk transactions and establishing requirements and procedures adequate for carrying out such transactions.

(2) The Company may consider such transactions to be low risk transactions which are not anonymous and where the obligated person is upon the suspicion of money laundering or terrorist financing able to apply immediately the customer due diligence measures specified in Article 20 (1) of the Money Laundering and Terrorist Financing Prevention Act.

Criteria of low risk for person or customers

Upon identification and verification of persons or customers specified in Article 34 (2) 1)—4) of the Money Laundering and Terrorist Financing Prevention Act, the following concurrent circumstances shall be considered as the criteria of low risk:

1) verification is possible on the basis of publicly available information;

2) ownership and control structure is transparent and certain;

3) activities and accounting practices are transparent;

4) the person or customer reports to and is controlled either by the authorities of executive power in Estonia or an EEA State, or other authorities performing public duties or by an EC institution.

Criteria of low risk for transactions

(1) Criteria of low risk for transactions may include the requirements that the benefits of the product or related transactions cannot be realized for the benefit of third parties, except in the case of death, disablement, reaching a predetermined advanced age, or similar events.

(2) Transactions related to units of a mandatory pension funds may be considered to be in conformity with low risk criteria.

Code of Conduct for the collection and preservation of data

1. Introduction

1.1. This Code of Conduct for the collection and preservation of data is prepared by Trade.io Payment Solutions OÜ, an Estonian private limited company, registered under registry code 14657028 whose legal address is Parda tn 4, Tallinn city, Harju county, 10151 (hereinafter the “Company”).

1.2. The Code of Conduct for the collection and preservation of data is prepared to comply with the Money Laundering and Terrorist Financing Prevention Act and other legal acts of the Republic of Estonia and applicable guidelines.

2. Security measures

2.1. The Company takes appropriate technical and organizational measures to meet the requirements of the applicable law.

2.2. The Company uses the following tools and best practices:

2.2.1. Ruby on Rails best practices for user authentication, password storage;

2.2.2. Cold storage of user funds (cryptocurrencies);

2.2.3. Hyper Text Transfer Protocol Secure (HTTPS), the secure version of HTTP, the protocol over which data is sent between client's browser and the website that the client is connected to;

2.2.4. Multisignature wallets for user funds, only specific employees can access;

2.2.5. Banking is done by a bank trusted by other bitcoin exchanges;

2.2.7. Checking the numbers in the database on every withdrawal;

2.2.8. Only authorized employees can access the multi-currency servers;

2.2.9. On 3 failed logins the account will be temporary blocked;

2.2.10. All user activities on the website will be logged and an email will be send on password / email change;

2.2.11. 2 (two) factor authentication;

2.2.12. 24 (twenty four) hours human control on the funds;

2.2.13. Instant alerts notifications on mobile and desktop for all developers;

2.2.14. Deploying a new code will always happen when every important developer is online;

2.2.15. Offices will keep secret (official address will be a mailbox) to prevent robbery.

3. Preservation of data used for identification

3.1. The Code of Conduct for collection and preservation of data provides requirements for the preservation of data and documents used for identification in cases specified in Article 20 of the Money Laundering and Terrorist Financing Prevention Act and other relevant data which shall allow for identification of at least the following information upon a later reproduction of the data in writing:

3.1.1. data specified in Article 21 (1) and Article 22 (1) of the Money Laundering and Terrorist Financing Prevention Act;

3.1.2. a copy of the document used for identification;

3.1.3. methods for and time and place of submission or update of the data and documents;

3.1.4. other data gathered during identification and a reference of whether the data was gathered for establishing a business relationship or for using another service that does not require the opening of an account;

3.1.5. the name and official title of the employee who conducted the identification or verified or updated the data.

4. Special requirements for preservation of data on transactions

4.1. The Code of Conduct for collection and preservation of data provides requirements for registration and preservation of data on transactions pursuant to the Money Laundering and Terrorist Financing Prevention Act, which shall allow for a written reproduction of at least the following information:

4.1.1. data on transaction and in case of payment order an explanation provided by the originator or the customer;

4.1.2. data on funds which are the object of the transaction, including a reference of whether these funds were received from an account or whether cash, cheques or other instruments were used.

5. Documents and data serving as basis for identification of natural persons

5.1. The Company shall identify a natural person and verify the person on the basis of a document specified in subsection 2 (2) of the Identity Documents Act or a valid travel document issued in a foreign country or a driving license complying with the conditions provided in subsection 4 (1) of the Identity Documents Act. In addition to an identity document, the representative of a person participating in a transaction shall submit a document in the required format, certifying the right of representation. A person below 7 years of age may be identified on the basis of a birth certificate specified in § 30 of the Vital Statistics Registration Act.

5.2. A copy shall be made of the page of an identity document submitted for identification which contains the personal data and a photograph. In addition, upon identification and verification of the persons specified in subsection (1), the Company shall register the following personal data:

5.2.1. the name and the representative's name;

5.2.2. the personal identification code or, upon absence of a personal identification code, the date and place of birth;

5.2.3. the name and number of the document used upon identification and verification of persons, and its date of issue and the name of the agency which issued the document;

5.2.4. the name of the document used upon identification and verification of the right of representation, and its date of issue and the name of the issuer.

5.3. On the basis of the information received from the person, the Company shall register the address of the place of residence and the profession or area of activity of the person. If a customer or a person participating in a transaction entered into in economic or professional activities is a natural person of a contracting state of the European Economic Area or a third country, the Company shall register the information about whether the person performs or has performed any prominent public functions or is a close associate or a family member of a person performing prominent public functions.

5.4. A person participating in a transaction performed in economic or professional activities, a person participating in a professional operation, a person using a professional service or a customer shall, at the request of the Company, submit documents and provide relevant information required for application of the due diligence measures specified in subsection 20 (1) of the Money Laundering and Terrorist Financing Prevention Act.

5.5. A representative of a legal person of a foreign country shall, at the request of the Company, submit a document certifying his or her powers, which has been notarized or authenticated pursuant to an equal procedure and legalized or authenticated by a certificate substituting for legalization (apostille), unless otherwise prescribed by an international agreement.

5.6. If the documents or data cannot be received, documents certified or authenticated by a notary public or authenticated officially may be used for verification of the identity of a person.

5.7. A person participating in a transaction or professional operation performed in economic or professional activities, a person using a professional service or a customer shall, at the request of the Company, certify the correctness of the submitted information and documents by signature.

6. Documents and data serving as basis for identification of legal persons

6.1. The Company shall identify a legal person and its passive legal capacity and verify the information obtained. Legal persons registered in Estonia and branches of foreign companies registered in Estonia shall be identified on the basis of an extract of a registry card of the relevant register and foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equal document, which has been issued by a competent authority or body not earlier than six months before submission thereof.

6.2. The document submitted for identification shall set out at least:

6.2.1. the business name or name, seat and address of the legal person;

6.2.2. the registry code or registration number;

6.2.3. the date of issuance of the document and the name of the agency which issued the document.

6.3. On the basis of the documents specified in subsection (1) or, if the aforementioned documents do not contain the respective data, on the basis of the information received from the representative of the legal person participating in the transaction, the Company shall register the following data:

6.3.1. the names of the director or the members of the management board or a body substituting for it and their authorization in representing the legal person;

6.3.2. the area of activity of the legal person;

6.3.3. telecommunications numbers;

6.3.4. the data of the beneficial owners of the legal person.

6.4. If the Company has information that a politically exposed person of another contracting state of the European Economic Area or a third country may be related to a customer or a person participating in a transaction entered into in economic or professional activities, the circumstances specified in subsection 20 (2) of the Money Laundering and Terrorist Financing Prevention Act shall be registered on the basis of the information received from the representative of the legal person in addition to the data.

6.5. An extract of the registry card does not have to be submitted if the Company has access to the data of the commercial register and the register of non-profit associations and foundations via a computer network.

6.6. If the document or data cannot be received, documents certified or authenticated by a notary public or authenticated officially shall be used for verification of the identity of a person.

7. Registration of transaction data

7.1. Upon identification and verification of a person, the Company shall register the date or period of time of entry into a transaction and a description of the content of the transaction.

7.2. The Company shall register the following data about a transaction:

7.2.1. the account type, number, currency and significant characteristics of the securities or other property;

7.2.2. the names of the payer and the recipient, the payer's personal identification code, and upon absence thereof, the date and place of birth or a unique feature on the basis of which the payer can be identified;

7.2.3. the transaction amount, the currency and the account number.

8. Preservation of data

8.1. The Company shall preserve the original counterparts or copies of the documents specified in § 21 and 22 of the Money Laundering and Terrorist Financing Prevention Act, which serve as the basis for

identification and verification of a person, and of the documents serving as the basis for establishment of a business relationship, for no less than five years after termination of the business relationship.

8.2. The Company shall preserve on any data medium the documents prepared with regard to a transaction and the documents and data serving as the basis for the notification obligations specified in Article 49 of the Money Laundering and Terrorist Financing Prevention Act for no less than five years after entry into the transaction or performance of the notification obligation.

8.3. The Company shall preserve the documents and data specified in subsections 1 and 2 of this section in a manner which allows for a full and immediate reply to enquiries received from the Financial Intelligence Unit or, pursuant to legislation, from other investigative bodies or a court.

8.4. If the Company makes, for the purposes of identifying a person, a query to a database that is part of the state information system the use of which is obligatory for the Company under the legislation in force, the obligation provided for in subsections 1 and 3 of this section shall be deemed complied with if the information about making the electronic query to the corresponding register can be reproduced over a period of five years after the end of the business relationship.

9. Changes to the Code of Conduct

9.1. The Company shall from time to time review these rules in order to comply with the applicable law.

Code of Conduct for the performance of the notification obligation and for informing the management

1. Introduction

1.1. This Code of Conduct for the performance of the notification obligation and for informing the management is prepared by Trade.io Payment Solutions OÜ, an Estonian private limited company, registered under registry code 14657028 whose legal address is Pärnu mnt 158-88, Tallinn city, Harju county, 11317 (hereinafter the “Company”).

1.2. The Code of Conduct for the performance of the notification obligation and for informing the management is prepared to comply with the Money Laundering and Terrorist Financing Prevention Act and other legal acts of the Republic of Estonia and applicable guidelines.

2. Notification obligation in event of suspicion of money laundering or terrorist financing

2.1. If upon performance of economic or professional activities or professional operations or provision of professional services, the Company identifies an activity or circumstances which might be an indication of money laundering or terrorist financing or an attempt thereof or in the event of which the Company

has reason to suspect or knows that it is money laundering or terrorist financing, the Company shall immediately, but not later than within two working days from identifying the act or circumstances or from the rise of the suspicion, notify the Financial Intelligence Unit thereof.

2.2. The Company shall immediately, but not later than within two working days of executing the transaction, notify the Financial Intelligence Unit of any transaction where the financial obligation exceeding 32,000 euros or an equal amount in another currency is performed in cash, regardless of whether the transaction is made in a single payment or several related payments.

2.3. The Company has the right to postpone the transaction or professional operation. If the postponement of a transaction may cause considerable harm, the transaction has to be entered into or if it may impede catching the person who possibly committed money laundering or terrorist financing, the transaction or professional operation shall be carried out and the Financial Intelligence Unit shall be notified thereafter.

3. Place and format of performance of notification obligation

3.1. The information shall be forwarded to the Financial Intelligence Unit of the contracting state of the European Economic Area in whose territory the Company is situated.

3.2. A notification shall be communicated orally, in writing or in a format which can be reproduced in writing. If a notification was communicated orally, it shall be repeated the next working day in writing or in a format which can be reproduced in writing.

3.3. The data used for identifying and verifying a person or, where necessary, copies of relevant documents may be appended to a notification.

3.4. The format for notification to be forwarded to the Financial Intelligence Unit and instructions for the preparation thereof shall be established by a regulation of the Minister of the Interior.

4. Confidentiality obligation of notifier

4.1. the Company, and a structural unit, a member of a directing body and an employee of the Company who is a legal person is prohibited to notify a person, the beneficial owner or representative of the person about a notification given to the Financial Intelligence Unit about the person and about precepts made by the Financial Intelligence Unit or initiation of proceedings under § 57 of the Money Laundering and Terrorist Financing Prevention Act. After a precept made by the Financial Intelligence Unit has been complied with, the Company may notify a person that the Financial Intelligence Unit has restricted the use of the person's account or that other restrictions have been imposed.

4.2. the Company may give information to a third party if:

4.2.1. the third party belongs to the same consolidation group or financial conglomerate as the Company and the undertaking is located in a contracting state of the European Economic Area or third country where requirements equal to those provided in this Act are in force, state supervision is exercised over fulfilment thereof and requirements equal to those in force in Estonia are applied for the purpose of keeping professional secrets and protecting personal data;

4.2.2. the third party acts in the same legal person or structure, which has joint owners and a joint management or internal control system, as the Company who pursues the profession of a notary public, attorney or auditor;

4.2.3. the information specified in subsection (1) concerns the same person and the same transaction which is related to several Company and the information is given by a credit institution, financial institution, notary public, attorney or auditor to a person operating in the same branch of the economy or profession and located in a contracting state of the European Economic Area or third country where requirements equal to those provided in this Act are in force, state supervision is exercised over fulfilment thereof and requirements equal to those in force in Estonia are applied for the purpose of keeping professional secrets and protecting personal data.

5. Relief from liability

5.1. The Company, its employee, representative or a person who acted in its name shall not, upon performance of the obligations arising from the Money Laundering and Terrorist Financing Prevention

Act, be liable for damage arising from failure to enter into a transaction or failure to enter into a transaction by the due date if the damage was caused to the person participating in the transaction made in economic or professional activities in connection with notification of the Financial Intelligence Unit of the suspicion of money laundering or terrorist financing in good faith, or for damage caused to a customer or a person participating in a transaction entered into in economic or professional activities in connection with cancellation of a contract entered into for an indefinite period on the basis provided in subsection 42 (4) of the Money Laundering and Terrorist Financing Prevention Act.

5.2. The performance in good faith of the notification obligation arising from § 49 of the Money Laundering and Terrorist Financing Prevention Act and communication of relevant data by the Company is not deemed infringement of the confidentiality requirement provided by law or contract and no liability provided by legislation or contract is imputed with regard to the person who performed the notification obligation for disclosure of the information.

6. Guidelines of Financial Intelligence Unit

6.1. The Financial Intelligence Unit issues advisory guidelines to explain legislation regulating the prevention of money laundering and terrorist financing which is available on its website.

6.2. The Financial Intelligence Unit issues advisory guidelines regarding the characteristics of suspicious transactions which is available on its website.

6.3. The Financial Intelligence Unit issues advisory guidelines regarding the characteristics of terrorist financing which is available on its website.

7. Changes to the Code of Conduct

7.1. The Company shall from time to time review these rules in order to comply with the applicable law.

ANNEX 3: Risk assessment model in accordance with clause 14 subclause 1.6 of Money Laundering and Terrorist Financing Prevention Act for the application of customer due diligence measures

The following risks should be identified and managed through use of new and existing technologies, and services and products, including new or non-traditional sales channels and new or emerging technologies

I. Risks to users

Virtual currencies create numerous risks for users, and natural persons in particular. Some of these arise irrespective of the intended usage and purpose of holding or buying VCs, while others are specific to VCs used as a means of payment or as an investment.

1. Risks that arise irrespective of intended usage
The user risks in this category exist because of the technology underlying VCs and their general features.

1.1. User suffers loss when an exchange acts fraudulently (A01)

This risk arises when the conduct of employees of an exchange falls short of reasonable expectations by consumers; the exchange is not legally incorporated in a jurisdiction and cannot therefore be subjected to regulatory requirements; the corporate governance responsibilities of the exchange's senior management are unclear; and/or its business activities are not subject to an independent audit. The priority of this risk is high.

1.2. User suffers loss when the exchange they interact with does not exchange VC against FC (A02)

The risk can arise because anyone can anonymously create (and subsequently change the functioning of) a VC scheme. Anyone can set up and call themselves an exchange, and exchanges may not necessarily be registered entities subject to licensing or authorization requirements. The priority of this risk is high.

1.3. User experiences drop in value of VCs due to significant or unexpected exchange rate fluctuation (A03) Several different drivers can create this risk, including that VC markets, and the price formation therein, are relatively opaque, and that the VC price formation on exchanges can easily be manipulated, including by a concerted effort of a small number of large VC holders. Denial of service attacks may prevent processing of transactions, which can further exacerbate the problem. Finally, in the case of decentralized VC, there is, by design, no central authority that could intervene to stabilize exchange rates. The priority of this risk is high.

1.4. User holding VCs may unexpectedly become liable to tax requirements (A04)

The legal and regulatory treatment of VCs is unclear and inconsistent, as is their tax treatment. The taxable event and geographic location of the taxable event may also be unclear. This may potentially lead authorities to treat VCs as property, forcing users to track and pay capital gains. The priority of this risk is medium.

1.5. As a member of a VC mining pool, a user does not receive a fair share of mined VC units (A05)
The mining of VCs requires increased computing power over time, often exceeding that of a single computer. Users therefore have an incentive to mine VC units by pooling their computing capacity in a consortium.

However, a fair distribution of the mined units (or the equivalent in converted FC) to which each member is entitled might be subject to manipulation by the mining pool owner. Similarly, members might be exposed to other forms of unequal treatment, due to a lack of transparency in business practices.
Any automated, IT-based distribution mechanism may, in turn, be subject to errors, fraud and hacking, as is the verification of transactions that mining initially requires. No refund rights exist either, through which disadvantaged users would otherwise be compensated, nor can an incorrect distribution of VC units be revoked, as VC transactions are irreversible by design. The priority of this risk is low.

1.6. User suffers loss when buying VCs that do not have the VC features that the user expects (A06)

The inevitable lack of standards and definitions found in innovative products and services makes it difficult for users to gauge the features of a particular VC scheme. The units of the VC scheme bought may even transpire to be different from the expected scheme. The risk arises because anyone can anonymously create (and subsequently change the functioning of) a VC scheme, any computer file can be misrepresented as a VC and any scheme name can be given to that file, including the name of an existing, genuine VC. Once the user detects the misrepresentation, they

will be unable to reverse their decision as VC transactions are not reversible, the counterparties are anonymous, no legal contracts exist, and no complaints procedures are in place. The risk is of medium priority.

1.7. User's computing capacity is abused for the mining benefit of others (A07)

The mining and exchange of VCs is dependent on access to the internet and the processing power of personal computers (PCs), of which ever more is required over time to mine a VC unit. Both the internet and the PC have an unfavorable track record of protection against malware and other forms of hacking, making it feasible for a user’s PC to be infiltrated and its computing capacity to be misused for the mining benefit of others. The priority of the risk is low.

1.8. User suffers loss due to changes made to the VC protocol or other key components (A08)

The risk arises because anyone can anonymously create (and subsequently change the functioning of) a VC scheme. The software protocol that controls the VC scheme is not subject to any independent standards and can be changed once a majority of miners agree. These changes may accidently introduce errors, or miners may not necessarily act in good faith. The priority of the risk is high.

1.9. User is not in a position to identify and assess the risks arising from using VCs (A09) The decentralised and unregulated nature of VCs makes it difficult for users to access independent and objective information that would explain the risks arising from holding VCs. Some users may also have unfair information advantages, and the emergence of new VCs will affect the incumbents, and their prices, in unpredictable ways. The priority of the risk is low.

1.10. User is in violation of applicable laws and regulation (A10)

The regulatory and legal treatment of VCs is unclear and authorities may change their views unexpectedly, at short notice, and the view may not be communicated sufficiently. The priority of the risks is medium.

1.11. User suffers loss through e-wallet theft, hacking or soft/hardware malfunction (A11)

81. The risk arises because e-wallets are software that are stored on the user's computer or mobile devices. Those devices might suffer from malfunction as might the software itself. Furthermore, their encryption can be hacked, and unlike a conventional FC, this is possible from anywhere in the world. In many VC schemes, the e-wallet is stored unencrypted, making it an even easier target for hacking or theft. Furthermore, the user has no refund right after fraud because there are no safeguards in place, such as a deposit protection scheme for conventional accounts, and because lost or stolen coins cannot be distinguished from unused coins. The priority of the risk is high.

1.12. User suffers loss when exchange is hacked (A12)

An exchange may temporarily hold users' VC units but can be hacked. A user may suffer losses because of insufficient security measures implemented by the exchange, because the VC units were held in a separate account, because no own funds are available that could be used to repay users, because the user has no refund rights and because the transaction cannot be reversed. The risk priority is high.

1.13. User's identity may be stolen when providing identification credentials (A13)

Some VC schemes require users to identify themselves on the internet or at VC cash machines when buying/selling VCs, through passport scans, iris scans or finger printing. However, these identification measures are not subject to regulations or data protection laws, nor is the underlying IT software subject to safety standards. As a result, the user has no guarantee that the credentials they provided will be processed securely and only used for the intended purpose. Similar risks also arise for conventional payment transactions. The priority of the risk is high.

1.14. Market participants suffer losses due to unexpected application of laws that render contracts illegal or unenforceable (A14)

Until governmental and regulatory authorities have formed an opinion on VCs, legal uncertainty remains over any contractual relationships that market participants may have forged. Once authorities have formed a view, these legal contracts may be rendered illegal or unenforceable. The priority of the risk is medium.

1.15. Market participants suffer losses due to delays in the recovery of VC units or the freezing of VC positions (A15)

The risk arises due to the anonymity of (some) counterparties, the decentralized set-up of VC schemes, the fact that counterparties have insufficient own funds, and that VC markets become temporarily illiquid. The priority of the risk is high.

1.16. Market participants suffer losses due to counterparties/intermediaries failing to meet contractual settlement obligations (A16)

The risk arises due to the anonymity of (some) counterparties, which can undermine the enforcement of any legal contracts that may exist, the lack of 'payment vs. payment' procedures, the lack of settlement finality, the decentralized set-up of VC schemes, the fact that counterparties have insufficient own funds, and that VC markets become temporarily illiquid. The priority of the risk is high.

1.17. Market participants suffer losses of VC units held in custody by others (A17)

The risk arises because the custodian is insolvent, behaves negligently or fraudulently, lacks adequate governance arrangements to oversee transactions, fails to keep adequate records, or has inadequate own funds to repay creditors. Also, transactions are not reversible. The priority of the risk is medium.

1.18. Market participants suffer losses through information inequality regarding other market participants (A18)

The anonymity of some market participants and the lack of technological accessibility for others facilitate information inequality and insider know-how that are benefit the former and are to the detriment of the latter. The priority of the risk is medium.

2. Risks that arise when using VCs as a means of payment

2.1. User suffers loss when counterparty fails to meet contractual payment or settlement obligations (A21)

The risk arises because anyone can anonymously create (and subsequently change the functioning of) a VC scheme, no legal contract exists between the counterparties that could be enforced, the counterparties are not known to one another due to their anonymity, the counterparties have insufficient own funds to meet payment obligations, the payment service is not sufficiently reliable, the underlying IT security infrastructure is fragile, and no settlement finality exists. The priority of the risk is high.

2.2. User experiences loss of FC units when using a VC cash machine (A22)

When exchanging VCs for FCs at a VC cash machine, users cannot guarantee that the VC or FC units will be correctly credited to their benefit. This is because VC cash machines are not subject to harmonized technical specifications, nor are they subject to licensing requirements, and, when error or fraud occurs, VC transactions are not reversible. No effective complaints or redress procedures are in place either. The priority of the risk is medium.

2.3. User has no guarantee that VCs are accepted by merchants as a means of payment on a permanent basis (A23)

The risk arises because merchants are required to accept only legal tender in notes and coins, but they are not required to accept non-legal tender such as VCs. Furthermore, merchants may decide to vary the acceptance of alternative VCs over time, switching between various VC schemes. Merchants may also deem the overall costs and risks of VCs too high or too uncertain. The priority of the risk is high.

2.4. User suffers loss when the VC payment they have made to purchase a good is incorrectly debited from their e-wallet (A24)

The risk arises because no authority oversees the settlement process: instead the process is based on trust. Furthermore, if an error is detected, the transaction is irreversible, e-wallets may be hacked to conceal the error and no effective complaints and redress procedures are in place. The priority of the risk is high.

2.5. User is not able to convert VCs into FC, or not at a reasonable price (A25)

The risk can arise, for example, at an exchange where illiquid markets, low market depth, a lack of market makers and a non-fluid exchange can prevent arbitrageurs to operate and provide liquidity. More fundamentally, the risk can also arise because anyone can anonymously create (and subsequently change the functioning of) a VC scheme. The priority of the risk is high.

2.6. User cannot access their VCs after losing password/keys to their e-wallet (A26)

Unlike losing the password to your bank account, credit card or debit card, no central administrative entity may exist that could re-issue passwords. Additionally, no identity is attached to the e-wallet through which ownership could be proven. E-wallets can be hacked and no effective complains or redress procedures are in place. Although dependent on the amount at stake, the risk is deemed to be of high priority.

2.7. User cannot access their VCs on an exchange that is a going concern (A27)

The user may temporarily store their VC units on an exchange that is a 'going concern' i.e. is still functioning without an immediate threat of liquidation. However, they may find themselves unable to access them, because the exchange is not bound by any legal contract and is not subject to regulatory conduct and security requirements. The exchange can block the transfer of VC funds, FC funds or both, or may suffer from a lack of own funds. Furthermore, the transfers are not reversible. Although dependent on the amount at stake, the risk is of high priority.

2.8. User cannot access their VCs on an exchange that has gone out of business (A28)

Once an exchange has gone out of business, i.e. no longer has the resources needed to operate, users suffer because the exchange may have held insufficient own funds to satisfy the demands of its VC creditors, and the VC units may not have been held in a separate account in their name, but in that of the exchange instead. Furthermore, the status of VC creditors during bankruptcy proceedings and unwinding is also unclear. Whatever the causal drivers, users will have no right to be compensated for losses, nor are they protected by a scheme similar to a deposit guarantee scheme for conventional bank accounts. The priority of the risk is high.

3. Risks when using VCs as an investment

Individuals may use VCs not only as a means of payment for goods and services but also as an investment. The investment may take the form of holdings in VC units themselves or in investment products such as exchange traded funds (ETFs) or contracts for difference (CFD) that use VCs as an underlying asset. The risks arising from these activities are listed below.

3.1. User suffers loss as a result of VC prices being manipulated (A41)

The risk arises because of the low depth of VC markets; the ability of concerted action, by a small number of large VC holders, to undermine price formation; the general opaqueness of VC markets; and the absence of any central authority that could intervene to stabilize price formation. The priority of the risk is high.

3.2. User investing in regulated financial instruments using unregulated VCs as an underlying suffers unexpected loss (A42)

The risk arises because the lack of regulation of the underlying amplifies any risk taken on by purchasing the regulated investment product, such as a collective investment scheme (CIS), derivative or structured products. In addition, the investment products are highly complex, the returns are uncertain, and the underlying is opaque. The priority of the risk is medium.

3.3. User is misled by unreliable exchange rate data (A43)

100. The risk arises because the trading, market activity, market making, settlement and clearing on exchanges across the world are not subject to independent standards that would usually ensure there are reliable and consistent exchange rates. Furthermore, price formation in VC markets is opaque and subject to manipulation, and the execution of buy and sell orders lacks transparency. The priority of the risk is medium.

3.4. User suffers loss when investing in a fraudulent or Ponzi VC investment scheme (A44)

The risk arises because the individuals involved in the underlying asset can conceal their identity and are therefore not subject to any probity requirements, nor are they required to disclose the risks to which the investor is exposed, etc. Furthermore, the nature of VCs leaves investors more vulnerable to abuse by a Ponzi

scheme based on VCs than other, regulated forms of investments. Finally, the user may have no access to redress schemes. The risk is of medium priority.

3.5. User is exposed to significant price volatility within very short time frames (A45)

The risk arises because the trading, market activity, market making, settlement and clearing on exchanges across the world are not subject to independent standards that would usually ensure there are reliable and consistent exchange rates. Instead, the price of a unit of a particular VC scheme depends on the extent to which it is adopted and accepted as mainstream, which is uncertain. Furthermore, the market depth (i.e. the size of an order needed to move the market price by a given amount) is low, price formation in VC markets is opaque and subject to manipulation, and the execution of buy and sell orders lacks transparency. The priority of the risk is medium.

3.6. User cannot execute the VC exchange order at the expected price (A46)

The risk arises because VC exchanges tend to be cash poor. As a result, investors may find it difficult to sell the VCs when they want to, so as to prevent a loss or to make a profit. Furthermore, the low market depth gives rise to an increased execution risk, (i.e. that the order is not executed at the price expected by the user).

II. Risks to non-user market participants

Risks also arise to other, non-user market participants, such as exchanges, trade platforms, e- wallet service providers, merchants and others. Some of the risks apply to all participants, while others are specific to only one of them.

1. Risks specific to exchanges

1.1. Exchange is unable to fulfil payment obligations denominated in VCs or FCs (B11)

The risk affects the exchange and, consequently, also affects its creditors, because the exchange lacks adequate governance arrangements to oversee transactions, fails to keep adequate records, or possesses inadequate funds to repay creditors. Additionally, the particular VC that is being exchanged, and the underlying protocol that controls it, could be technologically faulty or compromised, or the IT environment

at the exchange itself could lack reliability or security. If the problem occurs once the exchange has defaulted, the risk arises because of insufficient financial safeguards against default and inadequate business continuity arrangements. The priority of the risk is high.

1.2. Exchange is not in control of its own operation (B12)

The risk affects exchanges and, consequently, also affects their creditors, because the exchange lacks adequate governance arrangements to oversee transactions, fails to keep adequate records, and operates within an IT environment that lacks safeguards against hacking and loss of control. The priority of the risk is medium.

1.3. Exchange suffers loss if refund policies are abused to hedge currency exchange transactions (B13)

If the exchange offers refund policies for VC transactions as a way to mitigate against one or more of the above risks, it may suffer losses as a result of other market participants abusing the policy to hedge VC currency exchange rate risks. The risk arises because of the high exchange rate volatility, and a transaction potentially taking a long time to be completed. The priority of the risk is medium.

2. Risks specific to merchants

2.1. After accepting VCs for payment, the merchant is not reimbursed (B21)

The risk arises because of the ‘double-spending problem’: unlike FC that has a physical representation in coins and notes, VC units are only digital files. Therefore, the act of spending a VC unit does not remove its data from the ownership of the original holder.

Electronic payment systems in FC prevent double-spending by having a central authoritative source that follows rules for authorizing each transaction. By design, no central authority exists in a VC scheme. To prevent double- spending, VC schemes tend to use a decentralized system with separate nodes that follow the same protocol. The authenticity of each transaction is verified by adding it to a transaction ledger, called the block chain, which is to ensure that the inputs for the transaction have not previously been spent.

However, there is no guarantee that a particular VC scheme uses this verification approach, nor is it certain that if this approach is used, it is completed securely and is not compromised, for example through 'blocking' individual users from the VC network. The priority of the risk is medium.

2.2. Unlike a FC, the merchant cannot be certain that they will be able to spend the VCs received (B22)

Once the merchant receives units that are denominated in a particular VC, there is no guarantee they will be able to spend them, for example, to pay invoices. VCs are not legal tender and therefore do not have to be accepted by other merchants, nor will the merchant be able to pay their tax liabilities in VCs. Acceptance of VCs depends entirely on the voluntary consent by other market participants, who may decide to vary the acceptance of alternative VCs over time, switching between various VC schemes. There is also no central authority that would act as a redeemer of last resort. The priority of the risk is medium.

2.3. The merchant cannot be certain of the FC purchasing power of the VCs they have received (B23)

The exchange rate between VC and FC fluctuates significantly, often within very short periods of time, and often due to unpredictable events, such as technological innovations or platform seizures. The purchasing power of a VC unit regarding goods and services denominated in a FC is therefore difficult to predict and exposes the merchant to exchange rate fluctuations. The priority of the risk is medium.

2.4. Merchant faces compensation claims from customers if transactions have been wrongly debited (B24)

E-wallet providers, exchanges, trade platforms and most other VC market participants are not regulated, and do not have a physical presence. Therefore, the VC scheme is not regulated either. Should an error emerge in a VC transaction, the aggrieved market participants may be left in a situation whereby the merchant is the only participant to whom a complaint and compensation claims could be addressed. More fundamentally, the risk arises because anyone can anonymously create, and subsequently change the functioning and core components of, a VC scheme. The priority of the risk is medium.

3. Risks specific to miscellaneous non-user market participants

3.1. E-wallet provider loses e-wallet provided to individuals (B31)

E-wallets are digital files and therefore are not only susceptible to hacking and other security breaches but, unlike conventional wallets, can be stolen from anywhere in the world. Furthermore, the digital nature of e-

wallets generates significant economies of scale, which in turn facilitates large-scale theft through internet hacking. The priority of the risk is high.

3.2. Administrator of a (centralized) VC fails to meet payment and other obligations (B32)

The risk arises to the administrator and, therefore, indirectly to its creditors. This is because an administrator of a centralized VC is in control of the VC scheme and its rules, but may change the rules, act without integrity, lack adequate and secure IT infrastructure and governance arrangements to oversee transactions, fail to keep adequate records, possess inadequate funds to repay creditors, or act with insufficient integrity (possibly leading to civil or criminal liability that leads to the discontinuation of the VC service). Should the risk materialize once the administrator has defaulted, the causal drivers are insufficient financial safeguards against default and inadequate business continuity arrangements. The priority of the risk is high.

3.3. E-wallet provider faces compensation claims from customers if the functionality of wallet is compromised or fails to provide expected features (B33)

The risk arises because of negligence on the part of the e-wallet service provider, inadequate governance arrangements, insufficient recordkeeping and lack of operational capacity. Additionally, e-wallet providers are not necessarily subject to legally binding terms and conditions with the user who holds the e-wallet. The user may therefore be misled about the functionality of its features, suffer a loss and will then seek to claim compensation from the e-wallet provider. The priority of the risk is medium.

III. Risks to financial integrity

Risks to financial integrity comprise risks of money laundering and terrorist financing, as well as financial crime. While the risks across these two categories are manifold, their causal drivers are often very similar and are primarily related to the anonymity and borderless nature of VCs, and the fact that anyone can create a VC, including criminals and terrorists.

1. Money laundering and terrorist financing risks

1.1. Criminals are able to launder proceeds of crime because they can deposit and transfer VCs anonymously (C01)

The risk arises because senders and recipients can carry out VC transactions on a peer-to- peer basis that do not require personal identification as there are no names attached to wallet addresses. Furthermore, there is no intermediary that could notify authorities of suspicious transactions. The priority of the risk is high.

1.2. Criminals are able to launder proceeds of crime because they can deposit and transfer VCs globally, rapidly and irrevocably (C02)

The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

1.3. Criminals or terrorists use the VC remittance systems and accounts for financing purposes (C03)

The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

1.4. Criminals or terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement authorities to obtain evidence and recover criminal assets (C04)

The risk arises because, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

1.5. Market participants are controlled by criminals, terrorists or related organizations (C05)

The risk arises because market participants are often led by individuals who are not ‘fit and proper’. The risk also arises because VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

2. Risks of financial crime

2.1. Criminals use VC exchanges to avoid regulated financial sector and trade in illegal commodities (C11)

The risk arises because senders and recipients can carry out VC transactions on a peer-to- peer basis that do not require personal identification, because there are no names attached to wallet addresses, and without the need for an intermediary that could be required to notify authorities of suspicious transactions.

In addition, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

2.2. Restorative justice for victims of crime is hindered by criminals using VCs to avoid seizure of assets and confiscation (C12)

In addition to the previously mentioned drivers of anonymity and the possibility for global and rapid peer-to-peer transactions, the risk is also caused by the possibility that law enforcement authorities are unable to target individual entities, as VCs do not require an intermediary (with the possible exception of exchanges). The priority of the risk is high.

2.3. Criminals can use VCs for anonymous extortion (C13)

The risk arises because senders and recipients can carry out VC transactions on a peer-to- peer basis that do not require personal identification, because there are no names attached to wallet addresses, and without the need for an intermediary that could be required to notify authorities of suspicious transactions.

In addition, as a means of payment, VC schemes are not confined to, and are accepted across, jurisdictional borders. VC transactions require nothing more than internet access, the VC infrastructure is often spread across globe, making it difficult to intercept transactions, and VC transactions tend not to be reversible. The priority of the risk is high.

2.4. Criminal organizations can use VCs for settlement of internal or inter-organizational payment needs (C14)

In addition to the previously mentioned drivers of anonymity and the possibility for global and rapid peer-to-peer transactions, the risk is also created because no interaction is required with the regulated financial system and the transactions are not monitored. The priority of the risk is medium.

2.5. VCs make it more feasible for individuals to engage in criminal activity (C15)
The anonymity of the creation (and subsequent changes to the function of VCs) combined with the easy access to VCs, the easy exchange between VCs and FCs, and the ability to avoid regulated financial systems makes it more feasible for individuals to engage in criminal activity, including the illicit purchase of goods and services and tax evasion. The priority of the risk is high.

2.6. The hacking of VC software, wallets, or exchanges allows a criminal to implicate others in the criminal activities that criminal commits (C16)

Criminals tend to use any means available to cover their tracks. Insufficient safeguards against the hacking and the lack of control of e-wallet providers, exchanges, trade platform and VC protocols allows a criminal to steal internet identities and therefore implicate others in the criminal activities they commit. The priority of the risk is medium .

2.7. Jurisdictions are able to avoid seizure of assets and confiscation, as well as international embargos and financial sanctions (C17)

VC transactions are not recorded and are anonymous, global and irrevocable. Also, decentralized VC transactions are not dependent on entities on which financial sanctions and embargoes could be imposed. As a result, it is difficult for governments and international governmental organizations to enforce financial sanctions or embargos against other jurisdictions, for example to further humanitarian objectives. The priority of the risk is high.

2.8. Criminals are able to create a VC scheme and use it for criminal purposes (C18)

Given the anonymity of the sender and the recipient of VC transactions, and of the inventor(s) of the VC scheme, criminals are able to create anonymously a VC scheme and ‘pre-mine’ a substantial share before the VC units are more widely released. As and when the currency has gained popularity and benefits from a higher exchange rate (which is potentially many years later), the criminals will possess substantial purchasing power, without ever needing to interact with FCs or to use an exchange. The priority of the risk is high.

2.9. Tax evaders are able obtain income denominated in VCs, outside monitored FC payment systems (C19) VC transactions are not recorded and are anonymous, global and irrevocable. Also,

decentralized VC transactions are not dependent on entities on which financial regulations could be imposed. The priority of the risk is medium.

IV. Risks to payment systems and payment service providers in FCs

The risks listed in this category cover issues that may potentially arise as a result of possible interdependencies between payment systems denominated in FCs and those denominated in VCs.

1. PSPs that use FC and also provide VC services suffer losses due to laws that render VC contracts illegal (D01)

Until governmental and regulatory authorities have reached an opinion on VCs, legal uncertainty remains over any contractual relationships that market participants may have forged. Once authorities have reached an opinion, these legal contracts may be rendered illegal or unenforceable, with associated impacts on the liquidity of the PSP. The priority of the risk is low.

2. PSPs that provide services in FC as well as VC fail to meet their contractual obligations as payment system participants due to liquidity exposures in their VC operations (D02)

The risk arises because of the decentralized setup of the VC system, the anonymity of (some) counterparties, VC counterparties failing to hold sufficient VC units to settle transactions, VC exchange price changing rapidly and the price formation not being transparent. Furthermore, the liquidity management of the PSPs may be inadequate; the need for liquidity may intensify, as well as potential operational problems in linking FC and VC (e.g. settlement failure, outages, capacity, fraud and data loss). The priority of the risk is low.

3. PSPs in FCs offering VC payment services suffer loss and reputational risk when providing unregulated VC services that subsequently fail to perform (D03)

This risk applies, in particular, to credit institutions that are also PSPs, as they may offer additional VC payment services to their existing banking customers, therefore implying that the product offered is also regulated. Should the VC services fail to perform as expected, the PSP risks its reputation and, possibly, suffers a financial risk too. The risk arises because PSPs have a legitimate incentive to innovate and provide

better value or lower costs offerings to consumers, and because consumers have trust in their banks and the products they offer. The priority of the risk is medium.

4. The overall economy suffers losses due to disruptions in financial markets that were caused by VC transactions and assets that were blocked or delayed, etc. (D04)

The risk arises in a scenario where VCs have grown to be so important that their non- functioning leads to unexpected credit and liquidity exposures of PSPs in VCs, which in turn delays VC and FC transactions to the detriment of the genuine business of the overall economy. The priority of the risk is low.

# Driver of risks	Risk(s) for which the driver is relevant
VC schemes can be created (and their functioning subsequently changed) by A02, A06, A08, A21, A25, B31, anyone, anonymously: Anyone can anonymously create a VC and can C05, C15, subsequently make changes to the VC protocol or other core components if the required majority of (anonymous) miners agree.	
Payer and payee are anonymous: Transmitters and recipients of VCs interact on a A01, A03, A05, A06, A21, B01, person-to-person basis but remain anonymous. B02, B03, B05, C01, C02, C03, C04, C05, C11, C12, C13, C14, C15, C17, C18, D01, D02, D03, E22,	
Global reach: the internet-based nature of VC schemes does not respect national C01, C02, C03, C04, C05, C11, and, therefore, jurisdictional boundaries C13, C17,	
Lack of probity: exchange is neither audited nor subject to governance and probity A01, B23, C04, standards, and is subject to misappropriation, fraud and seizure	
Not a legal person: market participants are not incorporated as entities that could A01, A02, C12, C17, be subjected to standards	

Opaque price formation: price formation on exchanges is not transparent and is A03, A41, A43, A44, A45, A46, not subject to reliable standards, and exchange rates differ significantly between B23, D02, D03 exchanges, which facilitates manipulation of exchanges
No refunds or payment guarantee: VC transactions are not reversible, so no A05, A06, A08, A 21, A22, A24, refunds are issued for erroneous transactions A27, A28, A29, A 43, B04
Unclear regulation: the regulatory treatment is unclear and creates uncertainty for A04,A10, B01, D01, E02,11, E22 market participants
Lack of definitions and standards: the features of a product can be A06, A42, misrepresented because of a lack of definitions and standards
j Inadequate IT safety: the IT systems, infrastructure, transaction ledger, VC protocol and encryption are either insecure, subject to fraud and manipulation, and, in the case of the protocol, can be changed through a majority of minders A07, A08, A11, A21, A22, A41, A42, B11, B12, B21, B31, C16, D01
Information is neither objective nor equally distributed: limited availability of A09, A41, A42,B05, B06, D03 comprehensible, independent and objective information on VC activities. As a result, some market participants benefit from information inequality, e.g. on events that influence price formation
Insufficient funds or VC units: market participants have insufficient funds to meet A21, A28, A29, A30, B04, B12, financial obligations or to compensate creditors in the case of bankruptcy D01, D02,
No separation of accounts: VC units temporarily held at an exchange are often not A27, A30, segregated from the exchange, i.e. held in client accounts
No complaint process: no effective channel for users to complain A06, A22, A42, B24, B33,

Lack of access to redress: no access to redress, compensation or protection A22, A28, A30, A42, A44, schemes

Lack of corporate capacity and governance: lack of skills, expertise, systems , A45, B04, B11, B12, B32, B33, controls, organizational structure and governance exercised by market participants E21
No reporting: lack of reporting requirements to any authority, e.g. of suspicious C01, C02, C03, C04, C11, C13, transactions C14, C16
Interconnectedness to FC: VC units and FC funds can be exchanged easily, D02, D03, D04, B05, therefore creating spill-over effects or risks from VC to FC systems
Not legal tender: merchants are not legally required to accept a particular (or any) A23 VC and can switch between different VC schemes
No stabilizing authority: no authority that could provide exchange rate stability A44, B22, and/or act as the redeemer of last resort

Internal Control Rules

This Internal Control Rules are prepared by Trade.io Payment Solutions OÜ, an Estonian private limited company, registered under registry code 14657028 whose legal address is Pärnu mnt 158-88, Tallinn city, Harju county, 11317 (hereinafter the "Company").

1. The tasks of internal control are:

1.1. to verify compliance of the Company and its managers and employees with the legislation, precepts of the Financial Intelligence Unit, decisions of the management bodies, internal rules, contracts and good practices concluded by the Company.

1.2. in co-operation with all the management levels of the Company, to identify and assess the risks that may affect the effectiveness of the Company's activities and its internal control system, determine the priorities of its activities and draw up work plans on the basis of the results of the risk assessment;

1.3. to assess the management and control measures implemented to achieve the Company's objectives, their effectiveness, sustainability and effectiveness, and express an opinion on the adequacy, reliability and necessity of these measures;

1.4. to inform the management board of its findings and conclusions and, if necessary, make recommendations for remedying the situation, modifying measures or implementing new ones;

1.5. as a result of the aforementioned activities, to increase the Company's management's confidence that the management and control measures implemented are aimed at achieving the goals set by the Company are sufficient and not superfluous.

2. The task of the management board of the company is to appoint a person responsible for the internal control of the Company (hereinafter: the internal auditor) and, if necessary, to set up a corresponding structural unit under the direction of that person, ensure the necessary conditions for the work of the internal auditor, access to the information necessary for work and the functional independence of the Company's other operations, and implement, as far as possible, proposals.

3. In order to ensure the independence of the internal control, the internal auditor shall not be involved in the duties that affect the outcome of an internal audit. The internal auditor's consultative activities are allowed.

4. The person responsible for internal control shall be independent in the planning of his activities.

5. The internal auditor shall be independent in carrying out audits, making observations, conclusions and recommendations, and informing the results, and maintaining neutrality with regard to the auditee.

6. Internal auditor requirements:

6.1. An internal auditor may be a natural person:

(i) who may not serve in the position and perform other duties which cause or may cause a conflict of interest;

(ii) who has impeccable reputation, honesty and high moral qualities, and who has the capabilities and personal qualities necessary for the work of the internal auditor;

(iii) having higher education.

6.2. The internal auditor is guided by the rules of conduct contained in internationally accepted standards.

6.3. The internal auditor ensures that the audits are carried out professionally and with due diligence, in accordance with applicable legislation and internationally accepted standards.

7. Risk Assessment, Audit Planning and Audit:

7.1. There is a risk that an event, activity or omission can cause loss of the assets or reputation of the Company and jeopardize the effective performance of the tasks assigned to the Company. The purpose of internal control is, among other things, to prevent the realization of risks, which will be achieved by fulfilling the work plan based on the results of the risk assessment.

7.2. Risk assessment for the purposes of this Procedure is a process aimed at identifying risks in the Company and prioritizing those changes that are necessary in the strategic audit plan, and preparing an annual work plan for an audit.

7.3. All the management levels of the Company and the person responsible for internal control must be involved in the risk assessment.

7.4. Risk assessment is carried out at least once a year before the audit work plans are drawn up.

7.5. An audit work plan is prepared for the planning of internal audit work.

7.6. The company's audit work plan is prepared by the person responsible for internal control and approved by the Management Board of the Company.

7.7. The audit work plan shall be prepared at the beginning of each year and shall state:

(i) the results of the risk assessment;

(ii) audit objects and objectives;

(iii) the planned deadline for completion of each audit by quarter;

7.8. The audit work plan must be based on the results of the risk assessment, take account of the operational priorities set for them and the resources available for internal audit, and leave a reasonable reserve to perform one-off tasks coming from the Company's management board.

7.9. An audit plan is prepared by the internal auditor. The audit plan must contain the following information:

(i) the purpose of the audit;

(ii) the name of the audited entity or sector;

(iii) the scope of the audit and the period covered;

(iv) the time of the audit;

7.10 The audit involves audit planning, audit activity, final report preparation and reporting of results and, if necessary, ex-post audits.

7.11. The audit object may be any of the Company's structural units, systems, processes, operations, functions and activities.

7.12 The internal auditor must be guaranteed access to the information necessary for conducting the entire audit in the Company.

7.13. The internal auditor shall be guaranteed all the rights and working conditions necessary for the performance of his duties, including the right to receive clarifications and information from the managers and employees of the Company, and to monitor the elimination of the deficiencies found and the implementation of the proposals made.

7.14. Internal audit is carried out at least 2 times a year.

8. Preparation and submission of a report:

8.1. At the end of each audit, the internal auditor will draw up an audit report, which will outline the findings, conclusions and recommendations for modifying the situation based on evidence contained in the audit dossier made during the audit.

8.2. The internal auditor shall forward the final report to the management board of the Company and, if necessary, to other management staff.

8.3. When reporting breaches of law, the internal auditor must comply with applicable laws and internationally accepted standards.

8.4. The Internal Auditor is required to promptly forward information to the Company's managers about the information disclosed to him about the violation of the law, or to the detriment of the interests of the clients.

9. Audit documentation and procedures:

9.1. Any information obtained during the audit, which is the basis for making conclusions and making recommendations, assessing risks and planning future audits, must be documented.

9.2. In order to ensure the high quality of the audit and to enable a later understanding of the audit process, all documents obtained during the audit and the prepared working papers must be included in the audit file. The dossier must ensure that the documents are easily accessible by reference in the final report and elsewhere.

9.3 The organization of internal control, the establishment and maintenance of audit dossiers must be guided by the laws and regulations governing the Company's current rules and procedures.