UCC ICO OÜ

Rules of procedure for prevention of money laundering and terrorist financing

Version 2.0

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

Rules of procedure for prevention of money laundering and terrorist financing (version 2.0)

Approved by a resolution of the management board on 11.08.2019

Table of contents

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

1. General provisions

1.1. These rules of procedure lay down internal security measures for conducting due diligence and detecting suspicious and unusual transactions in all areas of activity of our company.

1.2. All relevant employees should know and strictly follow the requirements set out in the Money Laundering and Terrorist Financing Prevention Act. The guidelines on the characteristics of suspicious transactions possibly involving money laundering and terrorist financing. Other guidelines on compliance with the Money Laundering and Terrorist Financing Prevention Act (MLTFPA) pertaining to the activities of the company as well as these Rules of Procedure and the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. Amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (AMLD5).

1.3. All relevant employees should keep themselves up to date with any amendments to the legislation and with other legal acts published on the website of the Financial Intelligence Unit (FIU) at: https://www2.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/

1.4. A copy of these Rules of Procedure shall be available to all relevant employees.

2. Definitions

2.1. What is money laundering?

2.1.1. Conversion or transfer of property derived from criminal activity, or, property obtained instead such property, knowing that such property is derived from criminal activity, or, from an act of participation in such activity, for the purpose of concealing, or disguising the illicit origin of the property, or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions.

2.1.2. The acquisition, possession or use of property derived from criminal activity, or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein.

2.1.3. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

2.2. What is terrorist financing?

The allocation or raising of funds to plan or perform acts which are deemed to be acts of terrorism or to finance operations of terrorist organisations, or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

2.3. What is a risk country?

Countries or regions of interest where the risk of money laundering or terrorism are high. A risk country is a country or jurisdiction that:

2.3.1. According to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective anti-money Laundering and combating the financing of terrorism (AML/CFT) systems.
2.3.2. According to credible sources has significant levels of corruption or other criminal activity.
2.3.3. Is subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations.
2.3.4. Provides funding or support for terrorist activities, or that has designated terrorist
organisations operating within their country, as identified by the European Union or the United Nations.

2.4. What is a high-risk country?

A country specified in a delegated act adopted on the basis of Article 9 (2) of Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The current list is available here:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.254.01.0001.01.ENG

.

2.5. Who is a politically exposed person (PEP)?

A natural person who performs or performed prominent public functions as well as their family members and close associates. Persons who, by the date of entry into a transaction, have not performed any prominent public functions for at least one year, as well as their family members or close associates shall not be considered politically exposed persons.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

2.5.1. For the purposes of these Rules of Procedure, the following persons shall be persons performing prominent public functions:

a) State, head of government, minister and deputy or assistant minister;
b) a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors, or of the board of a central bank;
c) an ambassador, a chargé d'affaires or a high-ranking officer in armed forces;
d) a member of an administrative, management or supervisory body of a state- owned enterprise;
e) a director, deputy director or member of the board, or equivalent function, of an international organisation, except middle-ranking or more junior officials.

2.5.2. The following persons are considered family members of a person performing prominent public functions:

a) The spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or a local politically exposed person;
b) a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person;
c) a parent of a politically exposed person or local politically exposed person.

2.5.3. The following persons are considered close associates of a person performing prominent public functions:

a) A natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person or a local politically exposed person;
b) a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person or local politically exposed person.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

2.5.4. The following persons shall be local politically exposed person

a) A person who is or who has been entrusted with prominent public functions in Estonia, another contracting state of the European Economic Area, or in an institution of the European Union.

2.5.5. How the relevant employee should check if the customer is a PEP

:

The relevant employee should make a research using the potential customer's full name. In case, there are several similar results, the relevant employee must use another identifier (date of birth etc.) to be sure that the result found matches with the potential customer.
To check the relevant employee should use generally known internet research engines and the databases the Company has access to. For example, the relevant employee is able to check the PEP status of the potential customer using the NameScan database available at:

https://namescan.io/FreePEPCheck.aspx

2.6. What is the MLTFPA?

The legal act that regulates the activities of credit and financial institutions, other undertakings and institutions specified in the Money Laundering and Terrorist Financing Prevention Act and the Financial Intelligence Unit, which involve the prevention of money laundering and terrorist financing. In Estonian:
Rahapesu ja terrorismi rahastamise tõkestamise seadus (RT I, 17.11.2017, 2)

2.7. Who is a customer?

A person or a legal entity who uses, or has used, one or several services offered by our company

2.8. Who is a relevant employee?

A person who is conducting KYC/AML measures about the customer in our company.

2.9. What is a business relationship?

For the purposes of these rules of procedure, a business relationship is a continued contractual relationship with a customer.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

2.10. What is a transaction monitoring?

Every single investigation conducted by an employee about a customer.

2.11. Who is an ultimate beneficial owner of a legal entity (UBO)?

Ultimate beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal entity or arrangement. Reference to “ultimately owns or controls” and “ultimate effective control” refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. This definition should also apply to beneficial owner or a beneficiary under a life or other investment-linked insurance policy. Without derogating from the above, UBO is a private individual owning or controlling more than 25% of a legal entity.

2.12. What is the Financial Intelligence Unit?

A separate structural unit of the Estonian Police and Border Guard Board that exercises supervision and uses enforcement powers of the state on the grounds and pursuant to the procedure prescribed by law.
Postal address: Rahapesu andmebüroo (RAB), Tööstuse 52, 10416 Tallinn;
email: rahapesu@politsei. ee
Web-based reporting form:

https://www2.politsei.ee/et/organisatsioon/rahapesu/saada-teade.dot

3. Standard procedure for customer identification and verification (on-boarding customers)

3.1. The relevant employee must identify all customers who wants to use our company’s services on the basis of an identity document and shall record the identification and transaction data regardless of whether the customer is a regular customer or not.

3.2. A person must be identified

a) Prior to establishing a business relationship;
b) upon suspicious customer behaviour;
c) upon verification of information or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered beforehand while updating relevant data.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

3.3. If the customer is a private individual, he or she must provide:

a) Their full name;
b) their personal identification code or, if none, the date and place of birth and the place of residence;
c) if the customer is in fact representing another private individual being the real customer (under a power of attorney, or in the case of inheritance, or any other way) information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer;
d) whether the customer is a politically exposed person (PEP), a family member of a PEP or a person known to be a close associate with a PEP.

3.4. The following valid documents serve as basis for identification:

a) An identity card;
b) a passport;
c) a diplomatic passport;
d) an ID card of the citizen of the European Union;
e) a driving licence if the document shows the name, photo or face image, signature or signature image and date of birth or personal identification code of its holder

3.5. In identifying a person, the relevant employee is obliged to check the validity of the identity document, make sure the person matches the information on the document and check the age of the person. If in doubt about the identity of the person, the relevant employee is obliged to request additional information about the person. Upon sending a document that does not match the person or is invalid, the relevant employee must refuse the customer registration and notify the Compliance Officer.

3.6. The relevant employee verifies the correctness of the customer data, using information originating from a credible and independent source for that purpose. Where the identified person has a valid document specified in section 3.4 or an equivalent document, the person is identified and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document, or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

3.7. If the customer is an Estonian legal entity (for example a company), it must provide:

a) The name or business name of the legal person;
b) the registry code or registration number and the date of registration;
c) the names of the director, members of the management board or other body replacing the management board, and their authorization in representing the legal person;
d) the details of contact information to the legal person.

3.8. The relevant employee identifies a legal person based on a registry card of a relevant register or a registration certificate of a relevant register, or another document equal to such card or certificate.

3.9. The relevant employee must identify the beneficial owners (UBOs) and, for the purpose of verifying their identities, taking measures to the extent that allows the relevant employee to make certain that he/she knows who the beneficial owners are, and understands the ownership and control structure of the customer, or of the person participating in the transaction.

3.10. The relevant employee verifies the correctness of the information of a legal entity, using the information originating from a credible and independent source for that purpose. When the relevant employee is able to verify the information through such direct access, the submission of the documents specified in section 3.8 does not need to be demanded from the customer.

3.11. If the customer is a foreign legal entity (for example a company), it must provide in addition to the information in section 3.7, a Commercial Registry (or Company House or similar, depending of the country of origin) extract for the legal entity authenticated by a public notary and/or legalized and/or certified with an Apostille, unless otherwise provided for in an international agreement also showing the rights of representation for that legal entity.

3.12. A representative of a legal person of a foreign country must, at the request of the relevant employee, for example when the right of representation does not appear in the submitted document/s, submit a document certifying his or her powers (a power of attorney), which has been authenticated by a public notary and/or legalised and/or certified with an Apostille, unless otherwise provided for in an international agreement

3.13. The relevant employee may ask additional information about the customer in case of any suspicion about the customer's identity information or the customer's behavior. Such additional information asked should be relevant to the raised risks which, when obtained, may prove that the risks are in fact explainable.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

4. Simplified and Enhanced Due Diligence Procedure

4.1. The company does not apply a simplified due diligence procedure in its' activity.

4.2. The relevant employee shall undertake enhanced due diligence (EDD) if there is a higher risk of money laundering or terrorist financing such as:

a) There are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
b) the customer is a politically exposed person (except for a local politically exposed person, their family members or a close associates);
c) the customer is from a high-risk third country or their place of residence or seat or threat of the payment service provider of the payee is in a high-risk third country;
d) the customer is from a risk country, or from a territory that's considered a low tax rate territory.

4.3. Other factors that are referring to a higher risk pertaining to the customer:

a) When there are unusual factors in the customer onboarding, or when there are unusual transactions patterns without clear economic or lawful purpose;
b) customer is a legal person or a legal arrangement, which is engaged in holding personal assets;
c) customer is a cash-intensive business;
d) the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
e) the ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.

4.4. Other factors that are referring to a higher risk pertaining to the product, service, transaction or delivery channel:

a) Products/services that favours anonymity;
b) payments received from unknown or unassociated third parties;
c) a business relationship is established without the customer or the customer's representative being physically met in the same place except when a document issued by the Republic of Estonia for digital identification of a person or another electronic identification system with assurance level 'high';
d) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

4.5. The relevant employee must identify what the risks are in every particular case and undertake all appropriate measures to mitigate those risks. Depending on the case, the relevant employee may apply one or several of the following due diligence measures:

a) Verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;
b) gathering additional information on the purpose and nature of the business relationship, transaction or operation and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
c) gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the ostensibility of the transactions;
d) gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship in order to rule out the ostensibility of the transactions;
e) making of the first payment related to a transaction via an account that has been opened in the name of the customer participating in the transaction in a credit institution registered or having its place of business in the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force.

5. Collecting data and record-keeping

5.1. Our company is obliged to keep all records about our customer and our customers' behavior in such a way that it can always be presented to inspectors checking the recorded transactions.
5.2. The relevant employee shall put his or her name and, if the document is in a paper format, his or her signature at the end of each entry.
5.3. The Compliance Officer is responsible for keeping all relevant data.
5.4. The personal data of a customer, a customer's transaction and other relevant information must be stored for no less than 5 years after termination of the business relationship.
5.5. If a customer fails to submit all necessary documents and relevant information, or, if on the basis of the documents provided the relevant employee has a suspicion that money laundering or terrorist financing might be involved, the relevant employee shall not make a transaction with that customer and shall immediately inform the Compliance Officer and record as many customer details as possible that will later help to identify the customer.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

6. Risk based approach

6.1. The relevant employee analysing the customer and his/her behaviour should undertake investigative efforts that are proportional to the risk and complexity of the case and collect evidence using observations gathered in the case.

6.2. If the relevant employee identifies any additional risks, they will need to conduct investigative research to understand these risks in the context of the case.

6.3. Additional evidence will be needed to support the review and understanding if additional risks are identified.

6.4. The following questions may help to determine whether a transaction is suspicious or whether there is a risk of money laundering or terrorist financing:

a) Is it inconsistent with the customer's known activities?
b) Is the size of the transaction inconsistent with the normal activities of the customer as determined at the initial identification stage?
c) Are there any other transactions linked to the transaction in question of which our company is aware of and which could be designed to disguise money and divert it into other forms of other destinations or beneficiaries?
d) Is the transaction rational for the customer?
e) Has the customer's pattern of the transactions changed?
f) Is the customer's proposed method of payment unusual?

7. Interaction with the customer

7.1. The relevant employee may always contact the customer to clarify the information given or ask for additional information which is needed for the customer identification, or to address the risks of the case

7.2. The relevant employee should not request unnecessary or irrelevant information. A request for additional information must be related to the risks of the case, and after receiving the customer's response; the relevant employee may close or report the case to the Compliance Officer. If the risk of money laundering or terrorist financing is very high, the relevant employee shall report the case to the Compliance Officer without asking additional information from the customer.

7.3. The relevant employee shall never express themselves using words that give a reason for the customer to understand that his/her activity is suspicious and may be a subject for further report to the Compliance Officer.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

8. Monitoring the business relationship

8.1. A transaction monitoring shall be initiated based on a behaviour trigger of the customer or manually by the relevant employee or by the Compliance Officer. A relevant employee must investigate every initiated case.

8.2. The relevant employee cannot be working on a case if the customer in question is a close person to that relevant employee, or a customer that is in any other way connected with that relevant employee.

8.3. The relevant employee should determine what the risks of the case are. Each risk should be addressed and documented.

8.4. The relevant employee must conduct a pre-research and check whether the customer was checked previously and what were the concerns earlier.

8.5. The relevant employee must conduct customer research to determine the customer's profile and identify the source and origin of the funds used in a transaction.

8.6. The relevant employee must conduct an activity research of the customer and determine whether it is in line with the customer profile or if the behaviour seems suspicious. Activity research includes all observations about the customer's behaviour and any red flags in the activity.

8.7. The relevant employee must conduct research on all the counterparties if it is applicable in the case.

8.8. The case review may vary on the evidence needed to be collected about the customer and his/her activity. The relevant employee should use a risk-based approach to address the risks proportionally.

8.9. The relevant employee must document all the findings about the customer and customer's behaviour, which support the decision of the relevant employee about closing or reporting the case to the Compliance Officer.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

9. Understanding the risk profile of the customer and the risks related to new and existing technologies

9.1. During the monitoring of the business relationship, the relevant employee must collect enough evidence to mitigate the risks alerted. For this reason, the relevant employee should research and use the following information:

a) Source of wealth or the source of fund of the transaction (employment status, role or title in a company, employer, approximate salary, additional source of income, industry type etc.);
b) the customer's age;
c) location of the customer and the customer's counterparties;
d) the history of the customer's transactions;
e) the type of transactions;
f) any negative information associated with the customer;
g) any factors that cause the customer to be considered a high risk;
h) the relationship between the customer and the customer's counterparties;
i) the relationship between the customer and customer's place of residence.
j) other information which helps to understand the customer, the customer's activity and its counterparties.

9.2. The relevant employee shall always be aware that new, existing and emerging technologies may give the customer a possibility to hide his or her real identity or to make a fraud. Therefore, the relevant employee shall assess the risk of new and emerging technologies and address them within the process of onboarding the client and within the transaction monitoring.

9.3. The relevant employee shall also collect information about the devices the customer uses and their location and add this to the customer KYC file.

9.4. The relevant employee shall also use proxy piercing to identify whether the user is attempting to hide their location and add this to the customer KYC file.

9.5. The relevant employee must cross-check the customer through the internal and external (e.g. Fraud.ee) databases of device fingerprints, address, name, email, ID code and all other data that is available in order to detect double registrations or multiple accounts of the customer.

9.6. The relevant employee shall record every virtual currency wallet address that is either used to deposit into or withdraw from the system. They shall all be added into the same virtual currency addresses cluster.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

10. Decision-making

10.1. After each case review, the relevant employee will make a final decision about whether to report the case to the Compliance Officer or close the case, based on the evidence collected for the case, and provide a final conclusion that supports the decision made.

10.2. While making a final decision, the relevant employee should:

a) Finish the research about the customer, the customer's behaviour and the customer's counterparties;
b) understand the evidence collected and look for indications of unusual activities;
c) consider each piece of evidence on its own and consider all evidence at the same time;
d) if two pieces of evidence contradict each other, look at them together;
e) identify which pieces of evidence have the greatest impact on your analysis;
f) Identify each piece of evidence that has the least impact on your analysis;
g) determine which theory is most strongly supported by the evidence.

11. Risk appetite and PEP's requirements

11.1. In order to allow a PEP to be the customer of ours, the following must be fulfilled:

a) An approval from our company's management board for establishing a business relationship with that person.
b) Take adequate measures to establish the source of wealth and source of funds, which are involved in the proposed business relationship.
c) Where a business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

11.2. The relevant employee shall refuse to onboard the customer or, if an account is already opened, block the account and report to the Compliance Officer in case the relevant employee finds out that:

a) The customer is accessing the service from a high-risk country;
b) the customer is under sanctions in the European Union or USA;
c) the customer is known to be accused with money laundering or terrorist financing.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

12. Reporting procedure of suspicious and unusual transactions

12.1. If the relevant employee has a suspicion that he or she may be dealing with a suspicious or unusual transaction, the employee shall promptly report this to the Compliance Officer. In addition to the above-mentioned transaction and customer data, the Compliance Officer should also receive the reason for reporting and identification information about the customer.

12.2. The relevant employee is not allowed to notify the customer about the fact that the customer has been reported to the Compliance Officer.

12.3. In case of any suspicion, the relevant employee must notify the Compliance Officer by filling out the special notification form. The Compliance Officer must consider each report to determine whether it gives rise to grounds for knowledge or suspicion. Where such suspicion is determined, a suspicious transaction report made by the Compliance Officer shall be sent to the Financial Intelligence Unit.

12.4. The relevant employee must report to the Compliance Officer when he or she discovers any suspicious customer's behaviour related to money laundering, including, but not limited to cases where:

a) The customer makes transfers to other persons in different countries that do not conform to the person's usual activities;
b) the customer informs that the funds will be withdrawn by a third party acting on his/her behalf and on his/her account;
c) the customer's profile does not conform to the nature of the transaction being executed by him/her.

12.5. In case of suspicion of terrorist financing, the relevant employee must identify the risk related to the customer and report to the Compliance Officer if the risks related to a customer cannot be reasonably mitigated or explained.

12.6. The risks of terrorist financing include, but are not limited to:

a) The individual was born in a high-risk country;
b) the individual is a citizen of a high-risk country;
c) the individual has a place of residence in a high-risk country or the legal entity is incorporated in a high-risk country;
d) the natural person is associated with a legal person or another entity registered in a high-risk country.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

13. A person in charge of the performance of the AML/CFT obligations

13.1. The designated management board member shall be in charge of the compliance with the MLTFPA and relevant guidelines.

13.2. The management board may appoint a Compliance Officer for performance of AML/CFT duties and obligations. The management board shall co-ordinate the appointment of the Compliance Officer with the FIU.

13.3. Compliance Officer is a person who acts as the contact person for the Financial Intelligence Unit ensuring the compliance with the measures put in place to prevent money laundering and terrorist financing at our company.

13.4. Compliance Officer shall have the following duties:

a) Checking compliance with the money laundering prevention requirements in our company and carrying out training for the employees.
b) Carrying out preliminary analysis of submitted reports about suspicious transactions and deciding whether or not to refer a report to the Financial Intelligence Unit.
c) Sending information to the Financial Intelligence Unit in the case of suspected money laundering and responding to queries and precepts made by the Financial Intelligence Unit.
d) Gathering information received from employees about suspicious and/or unusual actions, processing such information and keeping records pursuant to the prescribed procedure.
e) Notifying the management board in writing of any problems with compliance with these internal Rules of Procedural, guidelines and other legal acts and making periodic submission of written statements on compliance with the requirements arising from the MLTFPA.

13.5. The rights of the Compliance Officer:

a) Making proposals for amending these Rules of Procedure, AML policy, and any other policies of our company that are related to anti-money laundering and the prevention of terrorist financing.
b) Monitoring the activities of the employees in pursuing the measures to prevent money laundering and terrorist financing.
c) Receiving data and information required for performance of the duties of the Compliance Officer.
d) Making proposals for re-organising the process of submission of notifications of suspicious and unusual transactions.
e) Receiving training in the field.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

13.6. The Compliance Officer may send the information or data that have become known to him or her in connection with suspected money laundering only to:

a) The management board of the company or to an employee especially appointed by the management board.
b) The Financial Intelligence Unit.
c) A preliminary investigating authority in connection with criminal proceedings.
d) The court on the basis of a court ruling or judgement.

13.7. In the event of a well-founded suspicion concerning money laundering or terrorist financing, the Compliance Officer shall promptly report it to the Financial Intelligence Unit.

13.8. A report shall be sent to the Financial Intelligence Unit using the web-based reporting form at:
https://www2.politsei.ee/et/organisatsioon/rahapesu/saada-teade.dot

in writing, orally or through electronic means of communication. If a report is communicated orally, the Compliance Officer shall duplicate it in writing during the next day at the latest. Copies of the documents that serve as the basis for a transaction, as well as the data or copies of the documents used as the basis for identifying a person, shall be enclosed with the filled-in reporting form.

13.9. The customer shall never be notified about any report sent about him or her to the Financial Intelligence Unit.

13.10. If the activities of a customer are not, in accordance with these Rules of Procedure, fully classifiable as activities which are to be reported to the Financial Intelligence Unit, any future activities of such customer shall be under increased scrutiny. The Financial Intelligence Unit shall be notified immediately if there is a well-founded suspicion about the behaviour of the customer.

13.11. No company, employee, the Compliance Officer or any other person acting on behalf of our company shall be liable for any damage which may arise from non-completion or late completion of a transaction that is incurred by the customer because of suspicions about terrorist financing or money laundering that have been reported in good faith to the Financial Intelligence Unit.

13.12. Reporting to the Financial Intelligence Unit and sending relevant information shall not be deemed to be a violation of the duty of confidentiality laid down by law or a contract and no liability prescribed by legislation or a contract shall be attributed to those persons for disclosure of such relevant information.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732

14. Training for employees

14.1. The Compliance Officer or other expert in the field of anti-money laundering shall carry out the money laundering and terrorist financing prevention training for the employees of our company.

14.2. The Compliance Officer is responsible for carrying out regular training. Each relevant employee shall confirm their participation with their signature. It is recommended to organize
trainings when necessary, but not less than once per year.

14.3. The Compliance Officer is obligated to provide instructions and an introduction training to all new relevant employees pursuant to the prescribed procedure following the signing of the employment contract no later than within one week after the commencement of employment by the relevant employee and to make the new relevant employee
familiar with these Rules of Procedure against signature

14.4. The Compliance Officer has the right to submit proposals to the management board concerning what trainings should be made.

15. Violation of duty to register information and keep records

15.1. Any violation of the duty to register information and to keep records as prescribed by these Rules of Procedure and in the Money Laundering and Terrorist Financing Prevention Act shall be disciplined in accordance with the law.

16. Requests from the Financial Intelligence Unit

16.1. Upon the request of a supervision officer of the Financial Intelligence Unit, all necessary documents and information shall be provided to the inspectors immediately.

UCC ICO OÜ
Roosikrantsi 2-K636, 10119 Tallinn, ESTONIA web: unisoncash.io email: info@unisoncash.io
managing director: Dipl.W.Ing. (FH) Nino Marco Fiammingo commercial register: 14537732