ExFrame OU

ExFrame OÜ

Registry code 14929521

RULES OF PROCEDURE AND INTERNAL CONTROL RULES

for the Implementation of the Money Laundering and Terrorist Financing Prevention Act and International Sanctions

Actual update date		
Date of preparation	**01.11.2021**	
Planned date of next update		

Confirmed

01.11.2021

Dmitri Orlov

Contents

1. General provisions

1.1 These rules of procedure for prevention of money laundering and terrorist financing, and compliance with international sanctions) in order to prevent entering into deals involving suspected Money Laundering and Terrorist Financing, and to ensure identification and reporting of such.

1.2 The obligation to observe the Rules rests with Management Board members and employees of the Provider of service, including temporary staff, agents of the Provider of service who initiate or establish Business Relationship (as defined in section 2.6) (hereinafter all together called the Representative). Every Representative must confirm awareness of the Rules with the signature.

1.3 The Rules are primarily based on the regulations of Money Laundering and Terrorist Financing Prevention Act (hereinafter the Act) and International Sanctions Act (hereinafter ISA).

2. Definitions

Money Laundering – is a set of activities with the property derived from criminal activity or property obtained instead of such property with the purpose to: conceal or disguise the true nature, source, location, disposition, movement, right of ownership or other rights related to such property; convert, transfer, acquire, possess or use such property for the purpose of concealing or disguising the illicit origin of property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action; participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the actions referred to subsections 2.1.i and 2.1.ii.

Terrorist Financing – acts of financing of terrorism as defined in § 2373 and § 2376 of the Penal Code of Estonia.

International Sanctions – list of non-military measures decided by the European Union, the United Nations, another international organization or the government of the Republic of Estonia and aimed to maintain or restore peace, prevent conflicts and restore international security, support and reinforce democracy, follow the rule of law, human rights and international law and achieve other objectives of the common foreign and security policy of the European Union.

Compliance Officer or CO – representative appointed by the Management Board responsible for the effectiveness of the Rules, conducting compliance over the adherence to the Rules and serving as contact person of the FIU.

FIU - Financial Intelligence Unit of the Police and Border Guard Board of Estonia.

Business Relationship – a relationship of the Provider of service established in its economic and professional activities with the Client.

Transaction – cash flow or payment order or cryptocurrency wiring form a Client to the Provider of service.

Client – a natural or legal person, who uses services of the Provider of service.

Beneficial Owner – is a natural person, who:

- taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action,

operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.

Ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

- Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.

- In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations, settler or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

Politically Exposed Person or PEP - is a natural person who is or who has been entrusted with prominent public functions including a head of state, head of government, minister and deputy or assistant minister; 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; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organization, except middle-ranking or more junior officials. The provisions set out above also include positions in the European Union and in other international organizations.

- A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.

- A close associate of a person performing prominent public functions is 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; and 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.

Local Politically Exposed Person or local PEP – a natural person, who performs or has performed prominent public functions in Estonia, a contracting state of the European Economic Area or in an institution of the European Union.

Provider of service or Obliged Entity – ExFrame OÜ registry code 14929521, address Harju Maakond, Kesklinna linnaosa, Narva mnt 13, 10151, Tallinn, Estonia.

Management Board or MB – management board of the Provider of service. Member of the MB, as appointed by relevant MB decision, is responsible for implementation of the Rules.

Equivalent Third Country – means a country not a Member State of European Economic Area but applying an equivalent regime to the European Union corresponding (AML).

High-risk country – a country specified in the EU/OFAC restrictive measures (sanctions) and IMF Offshore financial centers ("tax havens)".
High-risk third/prohibited 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, amending Regulation (EU) of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141/73, 05.06.2015, pp 73–117).

- in the FATF under the "High-risk and other monitored jurisdictions".

Information regarding countries or regions risk assessment (Annex 4).

'Risk appetite' means the total of the exposure level and types of the obliged entity, which the obliged entity is prepared to assume for the purpose of its economic activities and attainment of its strategic goals, and which is established by the senior management of the obliged entity in writing.

Virtual currency - a value represented in the digital form, which is digitally

transferable, preservable or tradable and which persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010 or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same directive.

Virtual currency wallet service - a service in the framework of which keys are generated for customers or customers' encrypted keys are kept, which can be used for the purpose of keeping, storing and transferring virtual currencies.

Virtual currency exchange service - a service with the help of which a person exchanges a virtual currency against a fiat currency or a fiat currency against a virtual currency or a virtual currency against another virtual currency.

3. Description of activities of the Provider of service

3.1 The Provider of service is the provider of a service of exchanging of virtual currencies against virtual currencies, a virtual currency against a fiat currency, and vice versa.

3.2 The Provider of service is a subject to authorization by the FIU.

4. Compliance Officer

4.1 The MB shall appoint a CO whose principal tasks are to:

- monitor the compliance of the Rules with the relevant laws and compliance of the activity of the Representatives with the procedures established by the Rules;

- compile and keep updated the data regarding countries with low tax risk, high and low risk of Money Laundering and Terrorist Financing and economical activities with great exposure to Money Laundering and Terrorist Financing;

- carry out training, instruct and update the Representatives on matters pertaining to procedures for prevention of Money Laundering and Terrorist Financing;

- report to the MB once a year (or more frequently, if necessary) on compliance with the Rules, and on Transactions with a suspicion of Money Laundering or Terrorist Financing;

- collect, process and analyse the data received from the Representatives or Clients concerning suspicious and unusual activities;

- collaborate with and report to the FIU on events of suspected Money Laundering or Terrorist Financing, and respond to enquiries of the FIU;

- make proposals on remedying any deficiencies identified in the course of checks. The CO must meet all the requirements, prescribed by the Act, and appointment of the CO shall be coordinated with the FIU. If, as a result of a background check carried out by the FIU, it becomes evident that the CO's credibility is under suspicion due to their previous acts or omissions.

ExFrame has appointed a Compliance Officer:
Mr Dmitri Orlov
Email: dmitri.orlov@smartpayments.ee

5. Application of due diligence measures

- The Provider of service shall determine and take due diligence (hereinafter DD) measures using results of conducted risk assessment and provisions of national risk assessment, published on the web-page of the Ministry of Finance of Estonia and Money Laundering and Terrorist Financing Prevention Act of the Republic of Estonia.

- The Representatives shall pay special attention to the activities of Clients participating in a Transaction and to circumstances that refer to Money Laundering or Terrorist Financing, including to complex, high-value or unusual Transactions which do not have any reasonable economic purpose.

- Depending on the level of the risk of the Client and/or Transaction and depending on the fact whether the Business Relationship is an existing one or it is about to be established, the Provider of service shall apply either normal DD measures, simplified DD measures or enhanced DD measures. The Provider of service shall also apply continuous DD measures to ensure ongoing monitoring of Business Relationships.

- DD measures shall include the following procedures:

● Identifying the Client and verifying its identity using reliable, independent sources, documents or data, including e-identifying;

● Identifying and verifying of the representative of the Client and the right of representation;

● Identifying the Client's Beneficial Owner;

● Assessing and, as appropriate, obtaining information on the purpose of the Business Relationship and the Transaction;

● Conducting ongoing DD on the Client's business to ensure the Transactions being carried out are consistent with the Provider of service's knowledge of the Client and its source of funds;

● Obtaining information whether the Client is a PEP or PEP's family member or PEP's close associate.

- The Provider of service shall establish the source of wealth of the Client, where appropriate (enhanced due diligence measures).

- To comply with the DD obligation, the Representatives shall have the right and obligation to:

- request appropriate identity documents to identify the Client and its representatives;

- request documents and information regarding the activities of the Client and legal origin of funds;

- request information about Beneficial Owners of a legal person;

- screen the risk profile of the Client/Transaction, select the appropriate DD measures, assess the risk whether the Client or another person linked with the Transaction is or may become involved in Money Laundering or Terrorist Financing;

- re-identify the Client or the representative of the Client, if there are any doubts regarding the correctness of the information received in the course of initial identification;

- refuse to participate in or carry out the Transaction if there is any suspicion that the Transaction is linked with Money Laundering or Terrorist Financing, or that the Client or another person linked with the Transaction is or could be involved in Money Laundering or Terrorist Financing.

- The objective of the continuously applied DD measures is to ensure on-going monitoring of Clients and Transactions. Conducting ongoing monitoring of the Business Relationship includes:

● scrutiny of Transactions being carried out to ensure that the Transactions being conducted are consistent with the Provider of service's knowledge of the Client, the business and risk profile of the Client;

● obtaining information on source of funds for Transactions;

● keeping up-to-date the documents, data or information, obtained during taking DD measures;

● paying particular attention to Transactions and Client's conduction, leading to criminal activity or Money Laundering or Terrorist Financing, and clarifying nature, reasons and background of Transactions;

● paying particular attention to the Business Relationship or Transactions, if the Client is from or the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries.

- Annual review of a Client being a legal entity is carried out regularly once a year. Updated data shall be recorded in the Provider of service's Client database.

- The Representative updates the data of a Client, who is either a legal person or a natural person, i.e. takes appropriate DD measures every time when:

● the Client addresses the Provider of service with the request to amend a long-term contract during the term of its validity;

● upon identification and verification of the information there is reason to suspect that the documents or data gathered earlier are insufficient, have changed or are incorrect. In this case, the Representative may conduct a face-to-face meeting with the Client;
● the data pertaining to the Transactions of Client reveal significant changes in the

Client's area of activity or business volumes, which warrants amending the Client's risk profile;

● the Provider of service has learned through third persons or the media that the activities or data of the Client have changed significantly.

- The Representative shall evaluate the substance and the purpose of the Client's activities, in order to establish the possible links of the respective Transaction with Money Laundering or Terrorist Financing. The evaluation should result in an understanding about the purpose of the Business Relationship for the Client, the nature of the Client's business, the risk levels of the Client and, if necessary, the sources of funds related to Transactions.

6. Risk Assessment and Risk Appetite

For the purpose of identification, assessment and analysis of risks of money laundering and terrorist financing related to their activities, the Management Board of the Company and, where necessary, the other Staff members engaged in mitigating the risks of money laundering and terrorist financing on a day-to-day basis prepare a risk assessment.

Upon preparation of the risk assessment, the Company maps the risks of money laundering and terrorist financing related to the provision of the virtual currency exchange service and the wallet service, taking into account the risk categories specified in clause 6.1. Thereafter the effects of the mapped risks on the activities of the Company are assessed and possible risk-mitigating counter-measures, their reasonableness and their applicability are analyzed.

Thereby it must be kept in mind that the steps taken to identify, assess and analyze risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of ExFrame OÜ.

As a result of the risk assessment, the following is established:

1) fields of a lower and higher risk of money laundering and terrorist financing;

2) the risk appetite, including the volume and scope of products and services provided in the course of business activities;

3) the risk management model, including simplified and enhanced due diligence measures, in order to mitigate identified risks.

Upon identifying a risk appetite, account must be taken of the risks that the Company is prepared to assume or that the Company wishes to avoid in connection with the economic activities as well as qualitative and quantitative compensation mechanisms such as the planned revenue, measures applied with the help of capital or other liquid funds, or other factors such as reputation risks as well as legal and other risks arising from money laundering and terrorist financing or other unethical activities.

The establishment of the risk assessment and risk appetite must be documented and, where requested/necessary, submitted to the Financial Intelligence Unit. The risk assessment and risk appetite are updated based on changes in the activities of the Company, but not less than on an annual basis.

The risks and risk threat arising from the activities of the obliged entity is stipulated under the Annex 5.

6.1 Determination of the risk profile

6.1.1 Determination of risk categories and factors increasing/reducing them

Upon determining customers' risk profiles, the Company takes into account the following risk categories:

1. risks relating to the customer/partner;

2. risks relating to countries, geographic areas or jurisdictions;

3. risks relating to products, services or transactions;

4. risks relating to communication or mediation channels or delivery channels of products, services or transactions between ExFrame OÜ and customers.

In the event of doubts in determining risk categories and controversial data regarding increasing and reducing factors of risk categories, the principle of a source of greater danger must be followed – where there are signs that place the customer/jurisdiction/product/service in a higher risk category, it should be relied on.

Customer risk or risk factors arising from the person or customer participating in a transaction, incl.:

1. the legal form, management structure, field of activity of the person;

2. whether the customer is a politically exposed person (PEP);

3. whether the beneficial owner who is a natural person is a third party;

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

5. the person is subject to an international sanction ;imposed by the United Nations, US (OFAC), EU;

6. a prior suspicion of money laundering and/or terrorist financing is known regarding the person;

7. the look and/or behaviour of the person are indicative of the person being a front;

8. whether the person participates in transactions where cash plays a great role (e.g., currency exchange locations, gambling operators);

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

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

Factors **increasing the customer risk** are, above all, situations where:

1. the business relationship is based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;

2. the customer is a cash-intensive business;

3. the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;

4. the ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.

Factors **reducing the customer risk** are, above all, situations where the customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner.

Geographic area / jurisdiction risk is a risk that arises from the country of the seat and/or place of business of the customer, incl.:

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

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

3. whether the country cooperates with a criminal group; whether criminal groups use the country for pursuing their operations;

4. whether the country engages in funding the spread of weapons of mass destruction;

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

6. whether international sanctions have been or are being imposed on the country.

Factors increasing the geographic risk are, in particular, situations where the person involved in a transaction or the transaction itself is connected with a country or jurisdiction:

1. that, according to credible sources, has not established effective AML/CFT systems;

2. that, according to credible sources, has significant levels of corruption or other criminal activity;

3. that is subject to sanctions, embargoes or similar measures issued by, for example, the European Union;

4. that provides funding or support for terrorist activities or that has designated terrorist organisations operating within their territory, as identified by the European Union.

Factors **reducing the geographic risk** are, above all, situations where the person participating in a transaction is from or the person's place of residence or seat is in:

1. a contracting state of the European Economic Area;

2. a third country that has effective AML/CFT systems;

3. a third country where, according to reliable sources, the level of corruption and other criminal activity is low;

4. a third country where, according to credible sources, AML/CFT requirements that are in accordance with the updated recommendations of the Financial Action Task Force (FATF) have been established, and where the requirements are effectively implemented.

The product, transaction and service risk is a risk that arises directly from the field of activity of the customer and from the nature of the services provided by the customer, incl.:

1. provision of gambling services in a casino, via the Internet as well as in sports events (betting);

2. sale of medicinal products;

3. sale of erotic and adult goods;

4. dating services;

5. sale of e-cigarettes and tobacco products;

6. private and personal banking;

7. currency exchange and forex trading;

8. purchase and sale of precious metals and stones;

9. purchase and sale of weapons;

10. pawnbrokers;

11. companies providing cross-border cash and securities transport service;

12. any other illegal field of activity (e.g., sale of narcotic substances, sale of banned goods, darknet goods and services, etc.).

Factors **increasing the product/service risk** are, above all, situations where:

1. a product that may favour anonymity is provided or a transaction that may favour anonymity is made;

2. payments received from unknown or unassociated third parties are involved;

3. a business relationship or transaction is established or initiated in a manner whereby the customer, the customer's representative or party to the transaction is not met physically at the same place and whereby § 31 of the MLTFPA is not applied as a safeguard measure;

4. new payment methods and new business practices, including a new delivery mechanism, or new or emerging technologies are used for both new and pre-existing products.

Factors reducing the product/service risk are, above all, situations where:

1. financial products or services that provide appropriately defined and limited services to certain types of customers, to increase access for financial inclusion purposes, are involved;

2. products whereby the risk of money laundering and terrorist financing is managed through other factors such as loading restrictions or the transparency of ownership (e.g., e-money of a certain type) are involved.

The risk related to the communication or mediation channels between ExFrame OÜ and customers is a risk that directly arises from the manner of communication with the customer and from the extent to which the given manner of communication allows for identifying the customer and verifying the correctness of the information submitted by the customer.

The risk related to communication channels is increased, above all, by the following factors:

it is a situation where communication with the customer takes place constantly via various channels, e.g., calls are made from telephone numbers of different countries, letters are sent from different email addresses, etc.

The risk related to communication channels is reduced, above all, by the following factors:

1. when communication with the customer takes place constantly via the same channels, using the same contact details that are also indicated for example in public registers / databases and/or on the customer's website or in the customer questionnaire.

6.2 Determination of the customer's risk profile

Upon determining the customer's risk profile, the risk categories (factors) and the factors increasing and reducing them must be taken into account. Upon determining the risk profile, all the risk factors must be taken into account as a whole and in terms of their mutual relationships. In the case of determining the risk related to customers, the Know Your Customer (hereinafter KYC) principle must be followed, i.e. the basis for determining the customer's risk profile is the information gathered upon application of due diligence measures. ExFrame OÜ divides its customers into **low-risk, medium-risk, high-risk and very high-risk customers**.

7. Identification of a person

Upon implementing DD measures the following person shall be identified:

- Client – a natural or legal person;
- representative of the Client – an individual who is authorized to act on behalf of the Client;
- Beneficial Owner of the Client;
- PEP – if the PEP is the Client or a person connected with the Client.

Upon establishing the relationship with the Client and when carrying out a Transaction, the Provider of service shall identify and verify the Client while being present at the same place as the Client or by using information technology means.

For identification of a Client and verification of the identity of a Client by using information technology means, the Provider of service shall use one of the following documents:

- a document issued by the Republic of Estonia for the purpose of digital identification;
- another electronic identification system within the meaning of the Regulation (EU) No 910/2014 of the European Parliament and of the Council2. If the Client is a foreign national, the identity document issued by the competent authority of the foreign country is also used simultaneously.

In case of identification of a Client and verification of the identity of a Client by using information technology means the Provider of service shall additionally obtain data from a reliable and independent source, e.g., identity documents databases.

7.1 Identification of a natural person

The identification and verification of the identity of a natural person must be carried out, as a general rule, in one step on the basis of an identity document.

A person should be identified on the basis of credible and independent sources. Credible and independent sources are, above all, various governmental IT solutions for verification of the validity of documents and verification of data as well as information obtained from various public registers. If the information gathered upon identifying a person cannot be verified from a credible and independent source, it is prohibited to establish a business relationship. Cooperation with a customer who is not willing to update their data required for identification may not be continued.

Upon identifying a customer who is a natural person, the following data must be collected and retained:

1. name;
2. personal identification code or, if none, the date and place of birth;
3. place of residence or seat;
4. contact details;
5. 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;
6. the purpose and nature of establishment of the business relationship;
7. beneficial owner, where prescribed by the Guide.

The identification and verification of the identity of a natural person is carried out on the basis of an identity document.

The following valid documents can be used as a basis for identification:

1. Estonian identity card;
2. Estonian citizen's passport;
3. a diplomatic passport;
4. a foreign citizen's passport;
5. an ID card of a citizen of the European Union;

Upon presentation of an identity document, the following should be verified:
1. validity of the document;
2. person's external similarity with the photo on the document;
3. The authenticity of the document must be checked. If there are any doubts, a member of the Management Board of the Company must be addressed and, to verify the authenticity of the document, a foreign mission of the country or the Ministry of Foreign Affairs must be contacted.

The identification of a customer is not a one-off step. The Staff must regularly update the customer's personal data and operation profile, ensuring that they are up to date. In view of the above, all the customers must undergo identification upon making a transaction, establishing a business relationship and during the business relationship.

Identification data must be updated. The Staff updates data obtained upon identification and verification of identity at least once every two years in the case of a low risk level (Tier 1), once per year in the case of medium risk (Tier 2) and twice a year in the case of high-risk levels (Tier 3).

To update data, the Staff takes the following steps:

7.1.1 verifies data in public databases and registers;

7.1.2 upon expiry of a document, contacts the customer and asks for a new version of the document. The document shall be provided within two months' time from the date of request.

If the customer is not willing to submit updated data upon expiry of the document, the Compliance Officer of the Company must be informed about it and the business relationship with them must be terminated as soon as practically possible.

7.2 Identification of a legal person

A legal person always acts via its management board or via a representative authorized by its management board. Upon identifying a legal person, it is important to identify the legal person as well as its representative.

Upon identifying a legal person, the following must be identified:

1. business name;

2. registry code;

3. seat and place of business;

4. data on the person's legal form and passive legal capacity;

5. names and authorization of the members of the Management Board;

6. details of the means of communication;

7. representatives' details;

8. politically exposed persons, if any;

9. data of beneficial owners.

The operation profile and purpose of operation of the person as a potential customer having a business relationship and the purpose of establishment and nature of the business relationship and other similar important information required for the establishment of a business relationship must be identified as well.

The identification and verification of the identity and passive legal capacity of a legal person is carried out, as a rule, on the basis of the data of the commercial register (in Estonia) or that of another equivalent register or a copy of the registration certificate or an equivalent document submitted in accordance with the procedure provided for in law.

Where the Staff has access to the commercial register, non-profit associations and foundations register or the data of the relevant registers of a foreign country via the computer network and is able to verify the data from a credible source, the customer does not need to submit a printout of the registry card. In such an event, the Staff makes a printout of the customer's registry card and records the data, indicating the date of making the printout.

If the customer is a legal person not established in Estonia, a printout of the customer's registry card must be requested. The registry card must have been issued in a language in which the Staff is proficient at a sufficient level (English, Russian, Ukrainian, Estonian).

Documents issued by a register or equivalent documents must have been issued not earlier than six months prior to their submission to ExFrame OÜ. In the case of doubt, the Staff may also demand a printout of the registry card authenticated by a notary or certified officially and/or having an apostille where a high-risk country or a high-risk profile customer is involved.

Upon identification of a legal person, it is also important to make a copy of the identity documents of the representatives of the legal person and to clarify the following data:

1. the names of the manager of a legal person, in the event of a foreign company the names of members of the management board or other body replacing the management board, and their authorization in representing the legal person;

2. the main field of activity of the legal person;

3. data of the beneficial owner.

In the case of foreign legal persons, the measures applied for identification must be as similar to those applied to Estonian legal persons as possible, but due to regulatory differences between foreign countries, it may not be easy or fully possible. Due to differences in the legislation of different countries, attention must be paid to, above all, companies established in countries or regions with a low tax rate, because it is not always abundantly clear whether they have passive legal capacity.

7.3 Identification and verification of the right of representation

The Staff must verify whether 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 obliged entity must also identify the person on whose behalf transactions are made. The employee must identify the basis, scope and term of validity of the representative's right of representation. The representative must be asked to submit a document proving the right of representation. Representation may be statutory or contractual (e.g., the authorization of a member of the management board to represent the company arises from law, while the authorization of the CEO of a legal person arises from a transaction/contract).

Documents required for identifying a legal person must be submitted by the legal representative or authorized representative of the legal person. The obliged entity must make certain that the right of representation complies with the requirements provided by law. If the submitted documents do not indicate the right of representation of the natural person submitting them and/or the authorization is not in compliance with the requirements, the identification process (and, thus, also the establishment of the business relationship and/or execution of the transaction) cannot be continued.

In the case of a contractual right of representation with authorization, the power of attorney should be requested and a copy thereof should be made. The power of attorney must be authenticated by a notary or certified by a notary. Clarification must 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 Staff must 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. For instance, if the authorized representative has the right to sign contracts and submit applications on behalf of the company on the basis of a submitted power of attorney, the authorized representative does not have any other unspecified rights and that must be taken into account upon provision of the customer with the service.

In view of the above, if a company is represented by someone other than a member of the management board, they should be asked for a document certifying their right of representation and the existence of their right of representation and the scope of their authorization should be verified, i.e., which actual steps the person is entitled to take on behalf of the represented company.

In the case of an authorized person or a legal representative it should be verified whether the representative knows the principal. It should be verified whether the representative knows:

1. the substance and purpose of the declarations of intent of the person represented by the representative;

2. the economic and professional activities of the principal;

3. the purpose of the transactions; the business partners of the principal;

4. the source and origin of the funds used in the transaction;

5. the circle of the owners of the legal person.

All the aforementioned data are important for making certain that the representative is indeed linked to the principal and acts in their interests.

7.4 Identification of a person using information technology means

It is possible to identify a customer using information technology means if the customer cannot be met face-to-face for the purpose of identifying the customer. As a rule, customers are identified using information technology means. Upon identification of a person using information technology means, the Company adheres to the Regulation "Technical Requirements of and Procedure for Identification of Persons and Verification of Data Using Information Technology Means" of the Minister of Finance.

A low-risk (tier 1/2/3) customer must, for the purpose of being identified and having their identity verified, submit:

1.a photo of the identity document;

2. a photo of their facial image (selfie) along with an identity document and date OR

video verification in the framework of which the person moves in front of the camera (liveness) after which it is made certain that the person in the video coincides with the photo of the person on the document.

Upon identification of persons and verification of identity (point 1 and 2 of the above) using information technology means, the photo (selfie) of a person must comply with the following requirements:

1. the person's head and shoulders must be visible;

2. the face must be clear of shadows;

3. the face must be clearly distinguishable from the background and recognisable;

4. the person may not wear sunglasses;

5. the face must be uncovered.

The identification can be carried out by the Staff of the Company as well as by using reliable companies providing verification services. Thereby the Company adheres to the rules provided for in § 24 of the MLTFPA concerning reliance on data gathered by other persons and enters into a written contract with such a person.

The Company uses the following partners for the performance of verification:

SUM AND SUBSTANCE LIMITED incorporated and registered in England with company number 09688671, whose registered office is at 80 Wood Ln, Central Working White City, London, United Kingdom, W12 0BZ

If identity document is submitted, attention must be paid to the following essential aspects, similarly to ordinary identity documents:

1. it must be made certain that the document type allows for establishing the person's identity;

2. it must be made certain that the document is valid;

3. The authenticity of the document must be checked. If there are any doubts, a foreign mission of the country or the Ministry of Foreign Affairs must be contacted to verify the authenticity of the

document, or a copy authenticated by a notary or certified officially must be requested or the document must be verified on the basis of any other reliable and independent source, using at least two different sources for verification of data in such an event.

The validity of the documents of EU Member States can be checked with the help of the Estonian register. The manual contains information on every country and the channels and websites through which the validity of the documents can be checked.

7.5 Identification of the beneficial owner of the Client

In the case of companies, a beneficial owner is the natural person who ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means.

'Direct ownership' is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

'Indirect ownership' is a manner of exercising control whereby a company that is under the control of a natural person holds or multiple companies that are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

Where no natural person holds or identifiably controls more than 25%, information must be requested about the shareholders, partners or other persons who exercise control or other significant influence over the activities of the legal person.

Where the documents submitted upon identification or other documents do not explicitly indicate who the beneficial owner of the legal person is, the relevant information is registered on the basis of a written document submitted by the representative of the legal person.

The Staff has the obligation to ask the data of the beneficial owner from the customer in the event of a legal person.

The correctness of the submitted data based on the written document of the customer is verified by taking reasonable measures. Among other things, queries are made to respective registers, the submission of the annual report of the legal person or the submission of another relevant document is requested. Upon acceptance of the document, the employee informs the customer of the liability arising from giving misleading or false information.

Upon determining the beneficial owner, the instructions given by the Ministry of Finance may be

of help. The instructions are available at:
https://www.rik.ee/sites/www.rik.ee/files/elfinder/article_files/tegelike_kasusaajate_andmete_esitamise_juhis.pdf.

Data on steps taken to identify the beneficial owner must be recorded.

7.6 Identification of Politically Exposed Person of their family member or a person known to be close associate

The Representative shall implement the following measures to establish whether or not a person is a PEP:

- asking the Client to provide necessary information;

- making an enquiry or checking the data on websites of the respective supervisory authorities or institutions of the country of location of the Client.

In a situation where a person participating in a transaction made in economic or professional activities, a person participating in a professional act, a person using a professional service, a customer or their beneficial owner is a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person, the Staff is required to apply the following due diligence measures:

1. request the required additional information from the customer, in order to identify the sources of wealth and funds used in the framework of the business relationship or transaction;

2. verify data or make queries to the databases of the public authorities of the country, and search for and verify data available on the internet.

The establishment of a business relationship with a politically exposed person is decided by the Management Board of ExFrame OÜ The Staff verifying the data informs the Management Board where a customer or beneficial owner later proves to be or becomes a politically exposed person.

In business relationships established with a politically exposed person, enhanced control is exercised regularly. Regular enhanced control must also be exercised after a politically exposed person has ceased to be a politically exposed person where, based on the risk-based approach, the person still entails a heightened risk.

Additional due diligence measures are applied to a politically exposed person at least 12 months after the person has stopped performing the prominent public functions conferred upon them.

'Local politically exposed person' means a person who is or who has been entrusted with prominent public functions in Estonia, another contracting state of the European Economic Area or an institution of the European Union. In the case of a local politically exposed person, usually the same additional due diligence measures as in the case of a politically exposed person are applied. However,

ExFrame OÜ has the right to omit the aforementioned additional due diligence measures where the customer is a local politically exposed person but other factors referring to a higher-than-ordinary risk are absent.

'Person subject to an international sanction' means a natural person or a legal person, authority, civil law partnership or legal arrangement explicitly specified in a legal instrument establishing or applying the international sanction and against whom measures provided for in the legal instrument establishing the international sanction are taken.

The Staff must pay special attention to the activities of a person having a business relationship with the Company or making a transaction or an act with the Company or planning the establishment of a business relationship or the making of a transaction or act with the Company as well as to factors referring to the possibility that the person is subject to an international financial sanction.

The Staff must:

1. upon establishment of a business relationship and making transactions, exercise special care towards the customer and the circumstances of the transaction (incl. with regard to the other party to the transaction);

2. in its activities, take notice of information on sanctions and respective lists on the website of the FIU (or use direct sources to that end);

3. report to the FIU on identifying a person subject to a financial sanction and on imposing the financial sanction on the basis thereof;

4. in the event of suspicion that a person is subject to a financial sanction, gather additional information (incl. from the customer);

5. in the event where the suspicion of the applicability of financial sanctions to a person or the circumstances of a transaction and another party persists after gathering additional information (also where no additional information can be gathered), report to the FIU on the suspicion, refusing to make further transactions and/or establish a business relationship until further notice;

6. report to the FIU on refusal to establish a business relationship or make a transaction where the basis for the refusal was a possible link between the person, state, transaction or goods that were the object of the transaction and an international sanction regime;

7. report to the FIU on a situation where there is a reason to suspect that a person is under the direct or indirect control of a person who is subject to an international financial sanction;

8. carry out checks for the purpose of identifying financial sanctions;

9. retain data related to financial sanction suspicions, impositions and checks.

If the Staff suspects or knows that a person having a business relationship with the Company or making a transaction with the Company is subject to an international sanction, the Staff immediately informs the Financial Intelligence Unit of identifying the person subject to the international financial sanction, the respective suspicions and the measures taken. In such a situation, the Staff is prohibited to establish a business relationship with the person or to make a transaction with the person and must immediately inform the Management Board and Compliance Officer of the Company of the fact.

8. Application of the Know Your Customer (KYC) principle

The Know Your Customer principle means the gathering of relevant information and data on the customer, including, in addition to identification of the person, the establishment of the customer's operation profile, the purpose of the customer's activities, the beneficial owner of the customer and, where necessary, the sources and origin of the funds used in the transaction, which allow the Company to assess whether the transactions made by the customer correspond to the customer's principal activity and/or payment habits and decide if the transaction is ordinary, suspicious or unusual.

It is important that ExFrame OÜ collects additional data in order to:

1. know who the customer is and what their ordinary activity is;

2. know the customer's actual contact details, citizenship, tax residency and field of activity;

3. make certain that the customer's transactions correspond to the nature and scope of the customer's economic activities.

Therefore it is important to keep in mind that, according to the Know Your Customer principle, additional information is requested not once, but it is a constant process of knowing and monitoring the customer. Therefore, the Company updates the data of its customers as follows:

1. in the case of very high risk customers, ongoingly;

2. in the case of high risk customers, at least once per a year;

3. in the case of medium risk customers, at least once per two years;

4. in the case of low-risk customers, at least once every three years.

To that end, the Company sends a questionnaire to its customer in order to make certain that the data are correct and valid.

To apply the Know Your Customer principle, the Staff must:

1. apply measures to identify the customer's field of activity and operation profile, incl.

2. ask data from the customer upon establishment of a business relationship or making a transaction;

3. check public databases and registers (e.g., the register of economic activities, the Tax and Customs Board, the commercial register, etc.);

4. if the employee in charge suspects the customer of money laundering or terrorist financing in connection with a low-risk transaction, enhanced due diligence measures must be applied.

The Know Your Customer principle is applied by sending the customer a questionnaire for collecting additional data and thereafter the submitted data are analyzed. Among other things, the Company assesses the changes in the customer's activities and whether the changes may raise the risk level so that additional due diligence measures need to be taken.

9. Monitoring a business relationship

A Staff member appointed by the Management Board of ExFrame OÜ undertakes to regularly monitor the business relationship with the customer in order to ensure that the transactions to be made correspond to the customer's risk profile.

To that end, the Staff member undertakes to:

1. monitor the size of the sums used in transactions and the frequency of transactions and, where necessary, identify the origin of the assets used in the business relationship and/or the transactions;

2. check the customer's legal status (existence of the passive legal capacity), financial situation and the field of activity, where necessary;

3. verify ownership information (beneficial owners);

4. checking of transactions made in a business relationship in order to ensure that the transactions are in consent with the obliged entity's knowledge of the customer, customer's activities and customer's risk profile;

5. regular updating of relevant documents, data or information gathered in the course of application of customer due diligence measures;

6. identifying the source and origin of the funds used in a transaction;

7. in economic or professional activities, paying more attention to transactions made in the business relationship, the activities of the customer and circumstances that refer to a

criminal activity, money laundering or terrorist financing or that is likely to be linked with money laundering or terrorist financing, including to complex, high-value and unusual transactions and transaction patterns that do not have a reasonable or visible economic or lawful purpose or that are not typical for the given business specifics. In the performance of these duties, it is necessary to ascertain the presence of these transactions, the reason and the background, as well as other information to understand the meaning and content of transactions, and to pay more attention to these transactions;

8. in economic or professional activities, paying more attention to the business relationship or transaction whereby the customer is from a high-risk third country or a country or jurisdiction specified in subsection 4 of § 37 of the AML/CFT Act or whereby the customer is a citizen of such country or whereby the customer's place of residence or seat or the seat of the payment service provider of the payee is in such country or jurisdiction.

In view of the above, in the event of long-term contracts, the Staff must send a questionnaire to the customer, have the customer fill it in and, thereafter:

1. verify whether the customer's risk data have changed;

2. verify whether the customer's geographic risk data have changed;

3. verify whether the customer's field of activity risk data have changed;

4. set/update the customer's risk profile.

9.1 Monitoring of the activity related to Fiat Currencies.

In order to accept fiat currencies, the Company uses the following channels:

- Single Euro Payment Area (or SEPA). Where the payments are settled to the

ExFrame OÜ accounts (IBAN) held in the Credit or Payment Institutions within the EU/EEA.

- Acquiring. Where the payments are settled to the ExFrame OÜ accounts held in the Acquiring banks within the EU/EEA.

The natural and legal persons are allowed to replenish the fiat accounts exclusively from their own accounts (under his/her names) opened in other Credit or Payment Institutions across the EU/EEA. Payments from third parties are strictly prohibited.

Supervision of the Customer's transactions is carried out by using the capabilities of the internal control system.

Description of the Internal control system and Fiat Currencies Monitoring principles are described in the Annex 6 **(the document is confidential, privileged, and only for the information of the compliance department employees and may not be disclosed without the consent of the MLRO).**

9.2 Monitoring of the activity related to Virtual Currency.

Monitoring of the Virtual Currency activity is performed with the use of the "Crypto Assets Analysis" tool provided by the SUM AND SUBSTANCE LTD (United Kingdom). The system performs analysis of connections that the address has with other addresses in the blockchain. This process also consists of screening customer's wallet addresses against available blacklisted wallet addresses as part of its ongoing monitoring.

This solution assists the Company effectively manage virtual currency transaction risk by identifying the 'risky' amount in the received sum. The 'Risky Amount' is the part of the transfer sum potentially received from criminal sources.

Moreover, the Company is required to monitor business relationships and to apply scrutiny of unusual, complex or high-risk virtual currency transactions or activity so that money laundering or terrorist financing may be identified or prevented.

The Company virtual currency transaction monitoring IT system monitors and establishes customer behaviour patterns in order to identify:
- a common wallet address is shared between accounts identified as belonging to two different customers;
- deposits into an account or address significantly higher than ordinary with an unknown source of funds, followed by conversion to currency of legal tender, which may indicate theft of funds;
- a customer conducts transactions with addresses that have been linked to darknet marketplaces or other illicit activity;
- a transaction makes use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces;
- a customer receives a series of deposits from disparate sources that, in aggregate, amount to nearly identical aggregate funds transfers to a known virtual currency exchange platform within a short period of time;
- any other activity, which the Company regards as particularly likely by its nature to be related to money laundering or terrorism financing.

Virtual Currency Transaction Monitoring principles are described in the Annex 7.

10. Standard due diligence measures

The Staff may not identify the customer in situation stipulated under the paragraph 6.2 of this procedure related to low-risk account, for the other means the company applying necessary due diligence measures listed below and in accordance with MLTFPA.

Where the customer's risk profile is low and medium risk, standard due diligence measures are applied to the customer and the following data are requested from the customer:

1. completed customer questionnaire (Annex 2);

2. verifying the identity document with use of information technology means;

3. verifying facial image (selfie) along with a document and date OR undergoing a liveness check with use of information technology means;

4. submission of a proof of residential address.

5. where the customer's place of residence or seat is in a country that has a central enrolment system, a certificate of enrolment and one month's utility bill not older than three months. Where the country does not have a central enrolment system, utility bills for three months, which are not older than three months. In addition to the above, it is possible to request a bank account statement of the last three months;

6. in the event of a legal person, extract from the commercial register (if the data are public, the Staff collects the data on their own, if the data are not public, the data are requested from the customer);

7. verification of whether the customer is a politically exposed person (PEP) or their spouse;

8. verification of whether the customer is included in the list of financial sanctions (European Union, FATF, United Nations) or embargoes;

9. a certificate or data concerning the beneficial owner;

10. in the event of a legal person, data about the beneficial owner (the data are requested from the customer);

11. verification of whether the customer is a politically exposed person (PEP) or their spouse;

12. verification of whether the customer is included in the list of financial sanctions (European Union, FATF, United Nations) or embargoes.

Where the customer's risk profile is high or very high risk apart from the measures described under the paragraph 10 (low and medium risk customers) an additional enhanced due diligence measures stipulated under the paragraph 11 shall be applicable.

11. Enhanced due diligence measures

ExFrame OÜ applies enhanced due diligence measures in order to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing. Enhanced due diligence measures are applied to high and very high risk customers.

The additional measures shall include request of the following data:

- a proof of funds wealth.

the customer must submit a certificate that confirms and proves the origin of funds obtained for the transaction.
Examples of valid source of funds are:

- recent payslip from your employers,
- sale contract of a personal asset (a house, a car, a company, etc.),
- bank statement (savings account extract, salary deposits, etc.),
- Heritage / gift (copy of the will, notarized letter, etc.),
- loan agreements,
- other supporting documents (a letter signed by a lawyer or a Notary Public, etc.)

In the event of a foreign document not drawn up in Estonian, English or Russian, the document must be translated to enable the Staff to examine the substance of the contract. In the event of a contract, it must be made sure that the contract is signed and valid. In addition to the above, the customer must submit a statement for the past three months issued by a credit institution;

Enhanced due diligence measures are applied always when:

1. upon identification of a person or verification of information submitted by the customer, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner(s);

2. a party to the transaction is a politically exposed person their family member or a close associate;

3. a party to the transaction is from a high-risk or tax heaven country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk or tax heaven country;

4. a screening result of the virtual currency transaction with use of “Crypto Assets Analysis” tool is medium-risk (25-75%);

5. a risk level determination decision prepared by the Staff has established that such factors amount to a higher-than-ordinary risk of money laundering or terrorist financing.

Where any risk-increasing factor arising from the customer, geographic area or transaction/service/product risk exists, enhanced due diligence measures need to be applied, i.e. each risk-increasing factor specified in Chapter 6.1 calls for the application of enhanced due diligence measures to the customer.

Upon application of enhanced due diligence measures, at least one of the following additional due diligence measures is applied:

1. identification of a person and verification of submitted information based on additional documents, data or information originating from a credible and independent source;

2. application of additional measures for the purpose of verifying the authenticity of documents and the data contained therein, among other things, demanding that they be certified by a notary or officially certified;

3. gathering additional information on the purpose and nature of the business relationship or transaction and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;

4. gathering additional information and documents regarding the actual execution of transactions and for the purpose of identifying the source and origin of the funds used in a transaction in order to rule out the ostensibility of the transactions;

Upon application of enhanced due diligence measures, the Company applies a dynamic level of risk evaluation which calculates on the daily basis. Dynamic risk is formed of initial risk level and other factors which are taken into consideration, such as transaction flow, customer behavior and others.

Upon emergence of an unusual transaction, act or factor, the Staff is required to analyze and compare the circumstances of the transaction with the characteristics of transactions suspected of money laundering and terrorist financing (see Chapter 13).

In view of the above, if there is a factor that refers to a possible low, medium or high-risk customer and enhanced due diligence measures need to be applied to the customer, the Staff undertakes to gather additional information in order to make certain that the making of transactions and the establishment of a business relationship with the customer is allowed and the customer is not suspected of being involved in money laundering or terrorist financing.

12. Establishing the purpose and actual substance of a Transaction

For the purpose of preventing movement of illegally obtained funds through the Provider of service it is essential upon entering into a Business Relationship, in addition to identification of the Client, to establish the business profile of the Client, which consists of mapping the main areas of operation

and possible payment practices. Notice is to be taken on persons that the Client has transactional relationships with, and their location.

It is necessary to bear in mind that certain circumstances, which are suspicious or unusual for one Client, could constitute a part of normal economic activities of another. Establishing the area of activity, work or profession of a Client allows assessing whether or not the Business Relationship or the Transactions are in conformity with the Client's normal participation in commerce, and whether the Business Relationship or the Transaction has an understandable economic reason for the Client.

In order to screen out suspicious or unusual Transactions and the purpose and actual substance of a Transaction, the Representative shall take the following actions:

- if necessary, ask the Client to provide (additional) information about the professional or economic activities;

- if necessary, ask the Client explanations about the reasons for the Transaction and, if necessary, documents evidencing of the origin of the assets and/or source of wealth;
- to verify if a customer conducts transactions with addresses that have been linked to darknet marketplaces or other illicit activity

- being particularly attentive to Transactions, which are linked with natural or legal persons, whose country of origin is a state, wherefrom it is particularly difficult to receive information about the Client and/or transactions with persons, who originate from such states, which do not contribute sufficiently into prevention of Money Laundering.

13. Identification of unusual transactions

The Staff of the Company undertakes to analyze the identification of a potential transaction suspected of money laundering where the following customer characteristics become evident in the course of their ordinary work:

1. the person wishes to use the services, but also to remain anonymous and conceal the (illegal) origin of the funds;

2. the person does not wish to disclose the beneficial owners;

3. the person who wishes to use the services of exchanging virtual currencies for fiat currencies or the virtual currency wallet services is suspected of being a front (e.g., their social appearance or background does not correspond to the nature of the commissioned service or business activity, the person cannot explain the service ordered or does not know facts about the activities of a business, etc.);

4. the person wishes, through the provider of the service of exchanging virtual funds for a fiat currency, to make transactions that lack any economic reason and on the basis of which it can be suspected that the business lacks actual economic activities;

5. the person refuses to give explanations on the transactions or the given explanations and documents are not plausible;

6. the person wishes to make a single transaction (or a series of linked transactions) with virtual currencies in an amount exceeding EUR 32,000 and does not wish to or does not provide convincing information on the origin of the assets;

7. the person contacts ExFrame OÜ with a proposal that has the characteristics of money laundering;

8. the person pays for a virtual currency from an unusual account (i.e. there is a reason to suspect that the person is not the account holder);

9. the person constantly uses different means of communication and channels to make contact;

10. the person provides a service that calls for an authorization, but the person does not have any authorization an attempt to perform a transaction from the other client's account that was not authorized by the account owner;

11. a single large-scale or regular purchase and sale of virtual currencies or payments for the use of other confidentiality-promoting financial instruments;

12. an Enhanced due diligence measures are (PEP) has purchased or sold virtual currencies on a large scale, exceeding the value of EUR 15,000;

13. in the case of a virtual currency transaction, technical means impeding the identification of the person are used;

14. assets worth over EUR 50,000 are purchased for a virtual currency;

15. the person pays for virtual currencies via an offshore account;

16. the person collects or transfers funds or a virtual currency to a person who is linked to terrorist organizations;
17. the person transfers funds or a virtual currency to a person or receives funds from a person who operates in a region where there is a high risk of terrorism.

18. the customer conducts transactions with addresses that have been linked to darknet marketplaces or other illicit activity or high risk or a screening result of the virtual currency transaction with use of "Crypto Assets Analysis" tool is high-risk (75-100%);

19. If any one of the aforementioned characteristics exists, the employee is required to apply additional due diligence measures and notify the Compliance Officer of the Company and the Compliance Officer, in turn, reports to the Financial Intelligence Unit. Reporting to the Financial Intelligence Unit is also necessary where no service is actually rendered to the customer and/or no business relationship is established.

Description of the Internal control system and Fiat Currencies Monitoring principles are described in the Annex 6 **(the document is confidential, privileged, and only for the information of the compliance department employees and may not be disclosed without the consent of the CO).**

14. Restrictions on transactions

It is prohibited to establish a business relationship or make a transaction:

1. in a situation where, based on documents collected in the course of application of due diligence measures to a business relationship, money laundering or terrorist financing or an attempt thereof is suspected;

2. where it is suspected that a person is subject to an international sanction;

3. where the customer wishes to settle in cash;

4. where a customer does not submit the documents and information required for compliance with due diligence measures (incl. information on the country of origin, field of activity, beneficial owner, etc.);

5. where, based on the data and documents submitted by the customer, there is suspicion of money laundering or terrorist financing or an attempt thereof, and the application of additional due diligence measures does not eliminate the suspicion;

6. where a customer fails to submit documents/data certifying the legal origin of the assets or a proof of residential address requested by the Company or any other document requested;

7. where a customer has not undergone the verification procedure successfully.

8. where a customer conducts transactions with addresses that have been linked to darknet marketplaces or other illicit activity.

In addition to the above, it is prohibited to make transactions with customers:

1. who are included in the list of sanctions;

2. who are included in the US embargo sanctions list;

3. who are citizens or residents of the country where trade in virtual currencies is not allowed;

4. who are citizens or residents of the country included in the list of prohibited countries (Annex 4);

5. who are citizens or residents of the country where trade in virtual currencies presumes the existence of additional authorizations.

ExFrame OÜ or the Staff is not allowed to:

1. make a transaction with a customer whose identity has not been established in accordance with this Procedure;

2. make transactions with persons who have the characteristics of a front;

3. make transactions with persons who hide data or submit false data;

4. make transactions with persons suspected of money laundering or terrorist financing before;

5. make transactions with persons who wish to settle in cash;

6. make transactions with persons included in the list of sanctions or embargoes.

Where there is a factor that does not allow for making a transaction or establishing a business relationship with a customer, as much data as possible on the customer's background and the origin of the assets must be obtained, the data must be recorded, the Management Board or Compliance Officer of the Company must be notified, and the Management Board or Compliance Officer decides whether it is necessary to report to the FIU.

15. Reporting of suspicious Transactions

In a situation where:

1. unusual circumstances become evident in a relationship with a customer or whereby the Staff has a reason to suspect money laundering or terrorist financing, or

2. circumstances prohibiting or precluding, in accordance with the Guide, the establishment of a business relationship or the making of a transaction become evident,

the Staff must immediately inform the Compliance Officer thereof. The Compliance Officer decides whether to report to the Financial Intelligence Unit and is responsible for reporting to the Financial Intelligence Unit without delay.

Upon performance of the duty to report, the Company adheres to the "Guidelines on the Characteristics of Suspicious Transactions" established by the FIU.

The Compliance Officer must inform the FIU immediately but not later than within two working days of the detection of the suspicion of money laundering.

The responsible Staff has the right to report to the FIU directly on the suspicion of money laundering or terrorist financing where:

1. a prior suspicion of money laundering and/or terrorist financing is known regarding the customer;

2. the customer has refused to submit data upon performance of the due diligence duty or has given false information and there is a reason to believe that failure to take immediate action could bring about negative consequences;

3. the customer has submitted forged documents and uses the name of another person;

4. the customer is subject to an international sanction.

The Staff must inform the Compliance Officer of the Company of, among other things, the following circumstances:

1. a business relationship cannot be established, a transaction or operation cannot be made or a service cannot be provided;

2. the establishment of a business relationship or the making of a transaction is refused due to the impossibility of the application of the due diligence measures;

3. the establishment of a business relationship or the making of a transaction is refused, because the person's capital comprises bearer shares or other bearer securities;

4. the customer does not, in spite of a respective request, submit documents and relevant information or data or documents proving the origin of the assets constituting the object of the transaction or, based on the submitted data and documents, there is a reason to suspect money laundering or terrorist financing.

The Compliance Officer analyses (and, where necessary, collects) information communicated by the Staff regarding the suspicion of money laundering or terrorist financing and reports it to the FIU.

Upon drawing up and sending a report to the FIU, the instructions on the substance and form of a report to be submitted to the Financial Intelligence Unit and the reporting instructions are followed.

The Management Board of ExFrame OÜ retains in a format that can be reproduced in writing all the reports received from the Staff about suspicious and unusual transactions as well as any information

collected for analysing these reports and other related documents and any reports forwarded to the Financial Intelligence Unit along with information about the time of the forwarding of the report and the employee that forwarded it.

It is strictly prohibited to notify a customer or a person participating in a transaction (incl. their representative and other related parties) with respect to whom a suspicion is being communicated to the Financial Intelligence Unit.

The report is forwarded to the Financial Intelligence Unit digitally, using the form on the website of the Financial Intelligence Unit (the "Send notification" link) or the format agreed with the Financial Intelligence Unit (XML format). A report in a format agreed with the Financial Intelligence Unit is forwarded via the information systems data exchange layer (X-road).

In the event of questions, the Financial Intelligence Unit must be contacted, using the following contact details:

Rahapesu Andmebüroo
Pronksi tn 12
10117 Tallinn
phone: 612 3840
e-mail: rahapesu@fiu.ee

16. Termination of the Business Relationship with a Client and cancelling a Transaction in the event of suspected Money Laundering and Terrorist Financing.

16.1 Pursuant to law, the Provider of service is obliged to extraordinarily and unilaterally terminate the Business Relationship and cancel all Transactions with the Client, without observing the advance notification period, if:

- the Client fails to present upon identification or upon updating the previously gathered data or the taking of DD measures, true, full and accurate information, or

- the Client or a person associated with the Client does not present data and documents evidencing of the lawfulness of the economic activities of the Client, or the legal origin of the funds used in the Transaction, or

- the Client uses fictitious persons to carry out the Transaction, or

- the Provider of service suspects for any other reasons that the Client or the person associated with the Client is involved in Money Laundering or Terrorist Financing, or

- the documents and data submitted by the Client do not dispel the Provider of service's suspicions about the Client's possible links with Money Laundering or Terrorist Financing.

The decision on terminating the Business Relationship and the activity of carrying out the Transactions shall be taken by the Management Board, considering also the proposal of the Compliance Officer.

The Client shall be notified of the termination of Business Relationship and cancellation of Transactions in writing. Notation about the cancellation of the Business Relationship shall be made in the Provider of service's Client database or documentation, and a note "AML" shall be added to the Client's data.

16.2 Indemnification of the Representatives.

The Provider of service and its Representatives shall not, upon performance of the obligations arising from the Rules, be liable for damage arising from failure to carry out a Transaction (by the due date) if the damage was caused to the persons participating in the Transaction made in economic or professional activities in connection with notification of the FIU of the suspicion of Money Laundering or Terrorist Financing in good faith, or for damage caused to a Client or a person participating in a Transaction carried out in economic or professional activities in connection with the cancellation of a Business Relationship and Transactions on the basis provided in Section 16.1.

Fulfilment of the notification obligation by the Representative acting in good faith, and reporting the appropriate information shall not be deemed breach of the confidentiality obligation imposed by the law or the contract, and no liability stemming from the legislation or the contract shall be imposed upon the person who has performed the notification obligation.

17. Implementation of International Sanctions

17.1 The Provider of service is required to implement International Sanctions in force (United Nations, US (OFAC), EU).

17.2 The ExFrame OÜ for the screened using reputable Due Diligence Databases (i. Member Check Pty Limited, NameScan) at the time of onboarding as well as for ongoing screening.

17.3 Representatives shall draw special attention to all its Clients (present and new), to the activities of the Clients and to the facts which refer to the possibility that the Client is a subject to International Sanctions. Control and verification of possibly imposed International Sanctions shall be conducted by the Representatives as part of DD measures applied to the Clients in accordance with these Rules.

17.3 The Representatives who have doubts or who know that a Client is subject to International Sanctions, shall immediately notify the Compliance Officer. In case of doubt, if the Compliance Officer finds it appropriate, the Representative shall ask the Client to provide additional information that may help to identify whether he/she is subject to International Sanctions or not.

17.4 The Compliance Officer shall be responsible for the implementation of International Sanctions.

The Compliance Officer shall:

- regularly follow the web page of FIU (https://www.fiu.ee/rahvusvahelised-sanktsioonid/rahvusvahelised-finantssanktsioonid) and immediately take measures provided for in the act on the imposition or implementation of International Sanctions;

- upon entry into force of an act on the imposition or implementation of International Sanctions, the amendment, repeal or expiry thereof, immediately check whether any of the Clients is subject to International Sanctions with regard to whom the financial sanction is imposed, amended or terminated;

- if an act on the imposition or implementation of International Sanctions is repealed, expires or is amended in such a manner that the implementation of International Sanctions with regard to the subject of International Sanctions is terminated wholly or partially, terminate the implementation of the measure to the extent provided for in the act on the imposition or application of International Sanctions;

- keep an updated record of subjects of International Sanctions and submit this information to the Representatives in the form that allows to use this information in the course of their activity;

- provide training to the Representatives that allows them to establish independently the subjects of International Sanctions;

- assist the Representatives if they have doubt or knowledge that a Client is a subject to International Sanctions;

- supervise the application of the Rules regarding the implementation of International Sanctions by the Representatives;

- review and keep updated the Rules regarding the implementation of International Sanctions;

- notify FIU of Clients who are subject to International Sanctions or in part of whom the Compliance Officer, the Representatives have doubts;

- keep record of made checks, notifications submitted to FIU and applied measures in part of detected subjects to International Sanctions.

When making checks on Clients as to detect whether they are subject to International Sanctions, the following information shall be recorded and preserved for five years:

- time of inspection;

- name of person who carried out inspection;

- results of inspection;

- measures taken.

If in the course of the check, it shall be detected that a Client or a person who used to be a Client is subject to International Sanctions, the Compliance Officer shall notify the Representatives who dealt with this Client, the Management Board and FIU. The notification shall be submitted at least in the way that allows its reproduction in writing.

The Client who is subject to International Sanctions and about whom the notification is made, shall not be informed of the notification.

Application of special measures and sanctions on the Client who is detected to be subject to International Sanctions should be authorized by FIU.

When making checks of Clients, the possible distorting factors in personal information (i.e. way of written reproduction of name etc.) must be kept in mind.

18. Collection, Verification and Retention of Data

ExFrame OÜ collects and retains data on a customer and persons related to the customer, which are learned upon performance of the due diligence duties.

The substance as well as the time or period of all transactions or steps are registered. Upon identification of a person and verification of submitted information, the respective step is registered as of the date or period of carrying out the verification.

Data on a transaction and a customer are registered based on a risk level determination decision.

ExFrame OÜ retains the originals or copies of the documents which serve as the basis for identification of persons and verification of submitted information, and the documents serving as the

basis for the establishment of a business relationship for five years after the termination of the business relationship.

ExFrame OÜ retains the documents and data on customers in a manner that allows for exhaustively and immediately replying to the enquiries of the Financial Intelligence Unit or those of other public authorities, among other things, regarding whether the Company has or has had in the preceding five years a business relationship with the given person and what is or was the nature of the relationship.

The Staff is required to retain:

- a copy of the identity document;

- responses to queries made to databases for the purpose of verifying data;

- questionnaires filled in by customers;

- all other documents or data that a customer has submitted in connection with the performance of the due diligence duties;

- the decision on determining the risk level;

- the consents and warranties of a customer (incl. on identifying the customer using information technology means);

- a report sent to the Management Board of the Company or to the FIU on suspected money laundering;

- decisions on / estimates of the reasons for refusal to establish a business relationship or make a transaction with the person.

When in doubt, the validity of the identity document must be verified on the website of the Police and Border Guard Board: https://www2.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/

ExFrame OÜ retains data received in the course of performance of the due diligence duty in a secure virtual server that has been leased (cloud service). Upon retention and processing of data, any and all terms and conditions and rules arising from the GDPR are adhered to.

Data associated with a suspicion of money laundering and terrorist financing are retained in a manner that does not allow for accessing it by anyone besides the Management Board of the Company or a person authorized by the Management Board.

ExFrame OÜ deletes the retained data after the expiry of a period of five years, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first-time limit.

The protection of personal data is of utmost importance and the Staff is required to adhere to the statutory rules related to personal data protection. The data obtained on the customer in connection with the performance of the employment duties are confidential and not subject to disclosure to third parties.

ExFrame OÜ may process the collected personal data solely for the purpose of preventing money laundering and terrorist financing and the data should not be processed in a manner that does not serve the aforementioned purpose.

Before the establishment of a business relationship or making a transaction, it is important to submit to the customer information concerning the processing of personal data.
Upon collection, processing and retention of personal data, the following must be adhered to:

the principle of lawfulness, i.e., personal data are collected and processed in strict accordance with legitimate purposes;

- the principle of minimalism, i.e., as little data as possible are gathered;

- the principle of data quality, i.e., the updating of the collected data;

- the principle of limited retention, i.e., data may not be retained for longer than necessary;

- the principle of security, i.e., data retention must be secure, using necessary technical and organizational measures.

In the event of questions concerning the collection, retention, processing or deletion of personal data, the Management Board of the Company must be addressed.

19. Training

The Provider of service shall ensure that all Representatives who have contacts with Clients or matters involving Money Laundering are provided with regular training and information about the nature of the Money Laundering and Terrorist Financing risks, as well as any new trends within the field. The CO shall arrange regular training concerning prevention of Money Laundering and Terrorist Financing to explain the respective requirements and obligations.

Initial training is provided at the start of representative service. The Representatives who are communicating with the Clients directly may not start working before they have reviewed and committed to the adherence of these Rules or participated in the Money Laundering and Terrorist Financing prevention training.

Training is provided regularly, at least once a year, to all Representatives and other relevant designated staff of the Provider of service. Training may be provided also using electronic means (conference calls, continuous email updates provided confirmation on receipt and acceptance is returned and similar means).

Training materials and information shall be stored for at least three years.

20. Internal audit and amendment of the Rules

Compliance with the Rules shall be inspected at least once a year by the CO. The report on the results of the inspection concerning the compliance with the measures for prevention of Money Laundering and Terrorist Financing shall set out the following information:

- time of the inspection;

- name and position of the person conducting the inspection;

- purpose and description of the inspection;

- analysis of the inspection results, or the conclusions drawn on the basis of the inspection.

If the inspection reveals any deficiencies in the Rules or their implementation, the report shall set out the measures to be applied to remedy the deficiencies, as well as the respective time schedule and the time of a follow-up inspection.

If a follow-up inspection is carried out, the results of the follow-up inspection shall be added to the inspection report, which shall state the list of measures to remedy any deficiencies discovered in the course of the follow-up inspection, and the time actually spent on remedying the same.

The inspection report shall be presented to the MB, who shall decide on taking measures to remedy any deficiencies discovered.

LIST OF HIGH-RISK THIRD/PROHIBITED COUNTRIES (RISK COUNTRIES)

From 23 October 2020

<u>High Risk Third/Prohibited Countries for ExFrame OÜ</u>

(Counties that are not acceptable according to the risk management system of the company. Not allowed to make a transaction or establish a business relationship)

FATF	EU
Albania Barbados	Afghanistan
Botswana	Bahamas
Burkina Faso	Barbados
Cambodia	Botswana
Cayman Islands	Cambodia
Ghana	North Korea
Jamaica	Ghana
Mauritius	Iran

Morocco	Iraq
Myanmar	Jamaica
Nicaragua	Mauritius
Pakistan	Myanmar
Panama	Nicaragua
Senegal	Pakistan
Syria	Panama
Uganda	Syria
Yemen	Trinidad and Tobago
Zimbabwe	Uganda
Iran	Vanuatu
North Korea	Yemen
	Zimbabwe

Tax havens and High-risk countries for ExFrame OÜ

(Transactions and establishment of a business relationship is possible only if additional due diligences procedures are applicable, Tier 2, Tier 3)

High-risk and “Tax havens” or IMF Offshore financial centers	
Tax havens	High-risk
Cyprus	Moldova
Malaysia	Bosnia and Herzegovina
Seychelles	Russia
Vanuatu	Turkey
Andorra	Egypt
Aruba	Ukraine
Bermuda	Cuba
British Virgin Islands	Lebanon
Cook Islands	Tunisia
Gibraltar	Belarus
Guernsey	Central African Republic
Isle of Man	Guinea-Bissau
Jersey	Burundi
Liechtenstein	Libya
Macau	Sudan
Monaco	South Sudan
Montserrat	Somalia
Netherlands Antilles	Guinea
Turks and Caicos Islands	Democratic Republic of the
Anguilla	Congo
Samoa	Mali
Palau	Venezuela
Belize	Iraq
Bahamas	Haiti

Countries listed under High Risk Third/Prohibited Countries are removed from this list.

ANNEX 6 . DESCRIPTION OF THE INTERNAL CONTROL SYSTEM AND FIAT CURRENCIES MONITORING PRINCIPLES

1. Description of the Internal Control System

Internal Control System – an electronic monitoring system designed to supervise the transactions carried out by the Customer in accordance with the parameters specified in the scenarios, in which is integrated the Company's Scoring System too. Company's Internal Control System seeks to identify, measure, monitor, evaluate and manage all risks of the Company. In this context, Internal Control System of the Company provides monitoring and control of the risks intrinsic to the activity of the Company either financial or non-financial, including risks in the areas of cryptocurrency, fiat money, client relationship and also operational, business and strategy, reputational, etc.

In addition to the Company's own IT solution, Internal Control System integrates third-party service providers independent solutions. For example, following services are being provided by Sum and Substance LTD: AML Screening, Identity Document Verification, Face Match and Liveness Check, Proof of Address Check, Legal Entities Check, Crypto Asset Analysis.

OU ExFrame Internal Control System features comprehensive and integrated policies and procedures, which are both quantitative and qualitative in nature. They are designed broadly to ensure measurement/control of risks, independent reporting with responsible behavior, as well as the respect for the adherence to regulatory and legal guidelines.

The Internal Control System is developed in accordance with strategies and policies defined by the responsible Board Member and MLRO.

The main objective of the Internal Control System is to ensure the following:
- Company's operations are efficient and effective;
- recorded transactions are accurate;
- financial reporting is reliable;
- risk management systems are effective;
- The Company complies with laws and regulations, internal policies and procedures.

The Internal Control System ensures the overall effectiveness of the Company. Monitoring of the risks on an ongoing basis is a part of the daily activities of the Company as well as periodic evaluations by the business lines and internal audit.

2. Monitoring principles of the fiat currencies

Supervision of the Customer's transactions includes the post-transaction and pre-transaction monitoring of transactions on the Customer's account. Supervision of the Customer's transactions is carried out in order to control:
- the compliance of transactions on the account with the personal activity planned by the

Customer and its volumes (on the basis of a customer's specific profile);

- the compliance of transactions on the account with the transactions previously performed by the Customer on the account;

- the existence of signs of Suspicious transactions (on the basis of detection rules and ongoing monitoring).

Transaction monitoring is conducted in combination of both real time (Pre-transaction monitoring) and after the event (Post-transaction monitoring), whereby transactions and patterns are reviewed after execution.

Monitoring Channels

In accordance with description provided in the Paragraph 9.1, acceptance of the fiat currencies is possible through the following channels:

- Payments made into the Company IBAN accounts held in the Credit or Payment Institution within the EU/EEA.

In this scenario the Company does not have a direct integration between its Internal Control System and the back office system of the Credit or Financial Institutions where the company held its accounts. Therefore, the Company is performing post-transaction monitoring which occurred after the event, whereby transactions and patterns are reviewed after execution. However, the Company is still able to prevent replenishment of the Customer account. The monitoring rules are developed and managed by the Company and implemented in the Internal Control System.

- Acquiring, where the payments are settled to the Company accounts held in the Acquiring bank within the EU/EEA.

In this scenario the customers can replenishment its account with use of Credit or Debit cards and considering the higher fraudulent risk of this channel, the Company implementing the post-transaction and pre-transaction monitoring which is being executed in real time, whereby transactions or activities are reviewed as they take place or prior to finalization (settlement). The monitoring rules are implemented on the Acquirer monitoring system upon the Company request.

4. **Monitoring Rules**

- **Monitoring rules which are related to Payments**

Rule Description	Required Action	Rule type	Payment status
- The Customer receive funds from the third-party account.	- Refund a payment	Post-transaction	Alert
- The Customer receives several payments with different name as beneficiary (especially commercial names).	- Refund a payment - Block the customer account; - Send SOF request with 3 days as due date. - Register AML Investigation;	Post-transaction	Alert
- The customer under low-risk account (Tier1) top-up his account above the applicable threshold	- Block the customer account (BLOCK) - Initiate full customer verification;	Post-transaction (limits are being monitored automatically)	Alert / Hold
- Fully verified customer top-up his account above the thresholds (Tier2, Tier3)	- Block the customer account (BLOCK) - Sent request to a customer and require providing necessary information within 3 days; - Register AML Investigation;	Post-transaction (limits are being monitored automatically)	Alert/ Hold

-High-risk customer (as an example - PEP) has purchased or sold virtual currencies on a large scale, exceeding the value of EUR 15,000	- Sent request to a customer and require providing necessary information (SOF) within 3 days; - Register AML Investigation;	Pre-transaction (limits are being monitored automatically)	Alert / Hold
- The Customer exceeded his limits to the maximum within 7 days after the account is opened	- Perform ongoing monitoring of the customer;	Post-transaction	Alert
- When negative information is obtained from reliable sources such as: - Banks and Financial Institutions; - Natural Person contacting support team claiming to be defrauded	- Block the customer account (BLOCK); - Request EDD measures. - Register AML_Investigation	Post-transaction	NA
- When negative information is obtained from reliable sources such as: 1. Police departments; 2. FIU; 3. Courts and other Authorities	- Register AML_Investigation; - Block the customer account (BLOCK) - Gather all information that is needed; - Prepare the STR.	Post-transaction	NA

-The person collects or transfers funds or a virtual currency to a person who is linked to terrorist organisations;	- Register AML_Investigation; - Block the customer account (BLOCK) - Gather all information that is needed; - Prepare the STR.	Pre-transaction	Decline

- **Monitoring rules which are related to Acquiring activity**

Rule Description	Required Action	Rule type	Payment status
- The Customer used card under third party name – single operation. The payments met any of the circumstances below: - Successfully and/or unsuccessfully; - Same and/or different BIN countries	- Refund a payment	Pre-transaction	Decline
- The Customer used more than 3 cards within a calendar day. The payments met any of the circumstances below: - Successfully and/or unsuccessfully; - Same and/or different BIN countries	- Block the customer account (DEBT_BLOCK) - Send request to a customer and require to provide necessary information within the 3 days; - Register AML_Investigation;	Post-transaction	Alert

- The Customer used more than 3 cards within a calendar month. The payments met any of the circumstances below: - Successfully and/or unsuccessfully; -Same and/or different BIN countries	- Block the customer account (DEBT_BLOCK) - Send request to a customer and require to provide necessary information within the 3 days; - Register AML_Investigation;	Post-transaction	Alert
- The Customer, successfully and/or unsuccessfully, used 1 or more cards from “unusual” or “unexplained” country(ies) other than the country of residence. - The BIN code is from an institution which does not open accounts for non-residents due to internal policy/national legislation. E.g.: 1. Latvian resident using Colombian cards; 2. Estonian residents using Turkish cards; etc.	- Block the customer account (BLOCK) - Sent request to a customer (template 1) and require to provide necessary information within 1 day; - Register AML_Investigation;	Pre-transaction	Alert
- The Customer has 3 or more top-ups denied with Base Anti-fraud on a calendar day.	- Block the customer account (BLOCK) - Sent request to a customer and require to provide necessary information within 1 day; - Register AML_ Investigation;	Pre-transaction	Alert
- The Customer used 1 or more cards to do several top-ups with high amounts in a very short period of time (especially during the night or weekends); - The activity is unusual or inconsistent with client’s activity.	- Block the customer account (BLOCK) - Sent request to a customer and require to provide necessary information within 3 days; - Register AML_ Investigation;	Pre-transaction	Alert
- The Customer used cards issued in High-risk	- Block the customer account	Pre-transaction	Alert

jurisdictions	(DEBT_BLOCK) - Send request to a customer and require to provide necessary information within the 3 days; - Register AML_Investigation;		
- The Customer used cards issued in Prohibited jurisdictions	- Block the customer account (BLOCK) - Sent request to a customer and require to provide necessary information within 3 days; - Register AML_ Investigation;	Pre-transaction	Decline
- The customer under DD top-up his account above the available limit	- Block the customer account (BLOCK) - Initiate full customer verification;	Pre-transaction (limits are being monitored automatically)	Alert / Hold
- Fully verified customer top-up his account above the thresholds	- Block the customer account (BLOCK) - Sent request to a customer and require to provide necessary information within 3 days; - Register AML_ Investigation;	Post-transaction (limits are being monitored automatically)	Alert / Hold

5. **Record keeping**

All information and documents received during the monitoring of the Customer are stored electronically in the Internal Control System. Information storage terms are stated in Paragraph 18. Collection, Verification and Retention of Data of this procedure.

ANNEX 7. VIRTUAL CURRENCY TRANSACTION MONITORING PRINCIPLES

1. General information

ExFrame OÜ (hereafter the "Company") performs transaction monitoring of the virtual currency operations and every transaction which is undertaken by a Client with the Company. This activity also shall be reviewed to ensure that they are in concert with the Client's initial declared scope and purpose for the establishment of the business relationship and coherent with the Client's Risk Profile and transactional history. Virtual Currency monitoring provides real-time risk assessment capabilities for evaluating and comparing risk associated with multiple blockchain transactions and their connections. The system gives a risk score based on blockchain interactions for a comprehensive assessment.

Said monitoring shall identify transactions which should be more thoroughly examined, based, among others, on frequency of transactions, forming or breaking of any pattern of behavior, size of the transaction, etc., taking into account the profile of the specific Client, and the observed characteristics of relevant groups of Clients.

Where a transaction is flagged as unusual or suspicious of ML/TF, the Compliance Function shall manually review the findings, assess the risks and operate according to its findings. After the aforementioned review is undertaken, the Risk Function shall document the transaction and the results of its review in the Client's AML File.

If the Risk Function determines that a transaction is suspicious of ML/TF, it shall provide a Report of Suspicion directly to the Company MLRO.

2. Systems description

2.1. Monitoring of Virtual Currency activity.

Monitoring of the Virtual Currency activity is performed with use of "Crypto Assets Analysis" tool provided by the **Sum and Substance Ltd** (hereafter the System). The System perform analysis of connections for both, incoming and outgoing addresses that has with other addresses in the blockchain and perform basic and enhanced checks:

- Basic check - every transaction screening starts with a basic check — address screening via API, with automatically generated risk profiles. The screening can result in one of three levels of risk: low risk (0-25%), medium risk (25-75%), high risk (75-100%). Low-risk transactions automatically pass the check, while high-risk transfers immediately fail it and get blocked. The levels of risk themselves are based on the intensity of their connections with the darknet market, payment processors, crypto exchanges and gambling services;

- Enhanced check - If the transaction is medium-risk (25-75%), it requires enhanced due diligence. Statistically, they are 10-15% of all transactions. The enhanced check allows compliance specialists to manually handle suspicious cases, evaluating each case for the percentage of their connections to suspicious market segments. The results are also viewed in relation to the transaction sum and the time it was made. The transaction made 2 years ago is much less risky than the one made a day ago. The evaluation largely depends on the internal policy of the business and they can decide whether to let the transaction be or block the users who initiated it from their business.

2.2. The System detects the following high-risk sources:
- **ATM** – cryptocurrency ATM operator (bitcoin kiosk).

- **Darknet Marketplace** – an online marketplace for trading illegal products using cryptocurrency.

- **Darknet Service** – an online organization offering illegal services in exchange for cryptocurrency.

- **Exchange With Low ML Risk** – exchanges that require KYC/AML identification for any deposit or withdrawal.

- **Exchange With Moderate ML Risk** – exchanges that allow daily crypto withdrawals of up to EUR 2000 in crypto daily without KYC/AML. KYC/AML is still required for fiat withdrawals.

- **Exchange With High ML Risk** – exchanges that allow daily crypto withdrawals of more than EUR 2000 in crypto daily without KYC/AML. (For fiat withdrawals, KYC/AML is required.)

- **Exchange With Very High ML Risk** – exchanges that don't use verification procedures or have requirements for certain countries only.

- **Fraudulent Exchange** – an exchange involved in illegal activity.

- **Gambling** – an online resource offering gambling services using cryptocurrency.

- **Illegal Service** – a resource offering illegal services or engaged in illegal activities.

- **Miner** – an entity that utilizes its computing power for mining cryptocurrency blocks.

- **Mixing Service** – a service that mixes funds from different sources in order to conceal their origin. They are primarily used for money laundering.

- **Online Marketplace** – an entity offering legal services/trading goods for cryptocurrency.

- **Online Wallet** – a service for storing and making payments with cryptocurrency.

- **Other** – none of the specified types. It may include a subtype.

- **P2P Exchange With High ML Risk** – P2P exchanges that allow daily crypto withdrawals of more than $1000 in crypto daily without KYC/AML procedures.

- **P2P Exchange With Low ML Risk** – P2P exchanges that require KYC/AML procedures for all deposits and withdrawals.

- **Payment Processor** – an intermediary overseeing payments between customers and businesses.

- **Ransom extortioner** – extortioners demanding payment in the form of cryptocurrency.

- **Scam** – entities that have scammed their customers and taken possession of their cryptocurrency.
- **Stolen Coins** – the entities which have taken possession of someone else's cryptocurrency by hacking.

2.3 Monitoring rules which are related to Virtual Currency transactions:

Rule Description	Required Action	Rule type	Payment status
Unusual cryptocurrency transaction types such as high frequencies in a short period of time - 5 or more crypto operations within 1hr on the amount greater than 1,000 euro or equivalent in virtual assets.	- Gather all information that is needed; - Register AML Investigation; - Prepare the UTR.	Pre-transaction	Alert / Hold
The customer moves cryptocurrency to or from high-risk countries or jurisdictions, or that sends currency to exchange in a country other than the one in which the customer is resident.	- Block the customer account (BLOCK); - Sent request to a customer and require providing necessary information (SOF) within 3 days; - Gather all information that is needed; - Register AML_Investigation;	Pre-transaction	Alert / Hold
Assets worth over EUR 50,000 are purchased for a virtual currency (single operation);	- Block the customer account - (BLOCK); - Sent request to a customer and - require providing necessary - information within 3 days; - Register AML Investigation;	Pre-transaction (limits are being monitored automatically)	Alert / Hold
The customer collects or transfers a virtual currency to a person who is linked to terrorist organizations;	- Block the customer account - (BLOCK) - Gather all information that is needed; - Register AML Investigation - Prepare the TFR.	Pre-transaction	Decline
High risk customer received virtual currency transaction with the score Medium risk 25 - 75%	- Register AML Investigation, Request SOF and inform MLRO	Pre-transaction	Alert/ Hold
Low/Medium risk customers received virtual currency transactions with the score high-risk.	- Block the customer account (BLOCK)	Pre-transaction	Decline

	- Initiate full customer verification; - Prepare the STR.		
Rapid deposit and withdrawal of funds into a recently opened account - Account registered within past 24hrs performed deposit and made withdraw of 80% - 100% of funds in 24hrs (and the amount of operation is above EUR 2,500 or in equivalent in virtual assets).	- Block the customer account (BLOCK); - Register AML Investigation; - Request SOF and inform MLRO	Pre-transaction	Decline
The high-risk customer has performed purchase in the amount of EUR 5,000 (and above) in the high-risk store such (high-risk MCC: jewelry, Cigar Stores and Stands,	- Block the customer account (BLOCK); - Register AML Investigation; - Request SOF and inform MLRO	Pre-transaction	Decline
The medium customer amount of transactions made between business partners, during the year, both incoming and outgoing payments for natural client increased by more than EUR 15,000 or in equivalent in virtual assets, and a monthly payment is more than EUR 2,000 or in equivalent in virtual assets and for legal client increased by more d EUR 25,000 or in equivalent in virtual assets, and a monthly payment is more than EUR 5,000 or in equivalent in virtual assets.	- Sent request to a customer and require providing necessary information (SOF) within 3 days; - Gather all information that is needed; - Register AML Investigation;	Pre-transaction	Alert/ Hold
Immediately withdrawing cryptocurrency deposits with no transaction activity	- Block the customer account (BLOCK); - Request SOF and inform MLRO	Pre-transaction	Alert/ Hold
New accounts funded with a large initial deposit from 32,000 euro or in equivalent in virtual assets, that is then traded or withdrawn in its entirety on that same day (or shortly thereafter)	- Sent request to a customer and require providing necessary information within 3 days; - Gather all information that is needed; - Register AML Investigation; - Prepare the STR.	Pre-transaction	Alert/ Hold
Frequent transfers of large amounts of crypto within a set period of time (day, week, month) to the customer account from more than one person.	- Sent request to a customer and require providing necessary information within 3 days; - Gather all information that is needed;	Pre-transaction	Alert/ Hold

	- Register AML Investigation; - Prepare the STR.		
Incoming small-amount transactions from unrelated wallets that are immediately transferred to another wallet or withdrawn for fiat currency.	- Sent request to a customer and require providing necessary information within 3 days; - Gather all information that is needed; - Register AML Investigation; - Prepare the STR.	Pre-transaction	Alert/ Hold
Multiple cryptocurrency transactions in the amount starting from 30 euros (that are deliberately structured in amounts that do not trigger reporting thresholds) or in equivalent in virtual assets.	- Sent request to a customer and require providing necessary information within 3 days; - Gather all information that is needed; - Register AML Investigation; - Prepare the STR.	Pre-transaction	Decline
Depositing into cryptocurrency wallets with funds that have been identified as stolen.	- Block the customer account (BLOCK); - inform MLRO; - Prepare the STR.	Pre-transaction	Decline
Funds deposited into a cryptocurrency wallet from a suspicious source, such as darknet marketplaces, gambling sites or other illegal sites.	- Block the customer account (BLOCK); - inform MLRO; - Prepare the STR.	Pre-transaction	Decline
The customer entering a cryptocurrency exchange from IP addresses associated with suspicious sources or conducting transactions with partners using encryption software.	- Block the customer account (BLOCK); - inform MLRO; - Prepare the STR.	Pre-transaction	Decline
High-risk customer (as an example - PEP) has purchased or sold virtual currencies on a large scale, exceeding the value of EUR 15,000 or in equivalent in virtual assets	- Sent request to a customer and require providing necessary information (SOF) within 3 days; - Register AML Investigation;	Pre-transaction (limits are being Monitored automatically)	Alert / Hold