FIATUM OÜ

Anti-money laundering and counter-terrorism financing ("AML and CTF") Policy

DOCUMENT OVERVIEW:

Version:	1.1
Created:	12.02.2021
Last updated:	27.07.2021
License type:	Virtual Currency Service Provider License (VCSP License)

Company name:	FIATUM OÜ
Company number:	14691717
Legal address:	Mäealuse tn 3a/3 Mustamäe linnaosa, Tallinn Harju maakond 12619, Estonia
Physical address:	Mäealuse tn 3a/3 Mustamäe linnaosa, Tallinn Harju maakond 12619, Estonia
Email:	director@fiatum.com
Website:	https://fiatum.com

Approved by:	Henrich Lipskij
Distribution:	Internal and to whom it may concern

Title:	AML and CTF Policy
Classification:	Internal
Status:	Approved
Version control:	1.1
Responsible person:	Henrich Lipskij

TABLE OF CONTENTS

INTERPRETATION

ABBREVIATION/TERM	DEFINITION
AML	Anti-Money Laundering
AMLD5	Anti Money Laundering Directive 5
Beneficial Owner (or BO)	Any natural person who ultimately owns or controls a customer and (or) the natural person on whose behalf a transaction or activity is being conducted. Beneficial owners include beneficial owners of corporate entities, beneficial owners of trusts and beneficial owners of legal entities such as foundations, or legal arrangements similar to trusts. Beneficial owners may own or control the customer through either direct or indirect ownership
Beneficial Owner of a Trust	The settlor, the trustee, the protector, the beneficiary and the person of other class, in whose main interest the trust is set up or operates, any other natural person exercising ultimate control over the trust by direct or indirect ownership by other means
Beneficial Owner of a Legal Entity such as Foundation, or Legal Arrangement similar to Trusts	The natural person holding equivalent or similar positions as the beneficial owner of a body corporate
Business Relationship	Any business, professional or commercial relationship which is connected with the professional activities of the customer and which is expected, at the time when the contact established, to have an element of duration
Business Sector with a High Risk of Corruption, or where Cash Transactions Have an Essential Role	Any of the following activities: forex trading, adult – related activities, unlicensed pharmaceutical, metallurgy, etc.
Cardholder	Cardholder is the client of merchant willing to make a payment for goods or services offered at the website
CDD (Customer Due Diligence)	Identifying and verifying the identity of the customer and any beneficial owner of the customer, and obtaining information on the purpose of intended nature of the business relationship
Company	FIATUM OÜ
Cryptocurrency	A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.
Criminal Conduct	Conduct which constitutes an offence in any part of

	Estonia, or would constitute an offence in any part of the Estonia if it occurred there
Criminal Property	Any money or other assets which constitutes a person's benefit from crime
CurrencyCloud	Engine with embedded Transaction Monitoring functionality
Direct Ownership	A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person
EEA	European Economic Area
Enhanced Due Diligence (EDD)	Additional customer due diligence measure that must be applied: • where the customer has not been physically present for identification purposes; • where the customer is a PEP or in any other situation which by its nature can present a higher risk of money laundering or terrorist financing
Enhanced Transaction Monitoring	Monitoring of customer transaction which is conducted additionally to transaction monitoring. The scope of transaction monitoring may include due diligence of all counterparties of the transaction, identification of their beneficial ownership and corporate governance structure, analysis of agreement, identification of the source of funds, examination of customs and tax declarations, etc.
EU	The European Union
Family members of PEPs	Any of the following persons: • the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; • the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person; • the parents of a politically exposed person
FIU	Estonian Financial Intelligence Unit
Fiat money	Fiat money is government-issued currency that is not backed by a physical commodity, such as gold or silver, but rather by the government that issued it.
Group	A group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other
Indirect Ownership	A shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person
KYB	Know Your Business

KYC	Know Your Customer/Client
Merchant	Merchant is online e-shop or web service that is offering its goods or services online via Internet
MLR	Money Laundering Regulations
MLRO	Money Laundering Reporting Office
MLTF	Money Laundering and Terrorist Financing
Nominated Officer	A Nominated Officer (also known as the MLRO officer) is the focal point within the company for the oversight of all activity related to anti-financial crime issues
Persons known to be close associates of PEP	Any of the following persons: • natural persons who are known to have joint 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; • natural persons who have 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
Politically Exposed Person	A natural person who is or who has been entrusted with prominent public functions, and includes the following: • heads of states, heads of governmental authorities, ministers and deputy or assistant ministers; • members of parliament or similar legislative bodies; • members of the governing bodies or political parties; • members of supreme courts, of constitutional courts or other high level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; • members of courts of auditors or the boards of central banks; • high ranking officers in the armed forces; • members of the administrative, management or supervisory bodies of state owned enterprises; • directors, deputy directors and members of the board or equivalent function of an international organization The definition excludes middle ranking or more junior officials
SAR	The suspicious activity report

Shell Company	A non-trading company used as a vehicle for various financial maneuvers or kept dormant for future use in some other capacity
Supporting Officer (s)	A person or persons nominated to act on behalf of the Nominated Officer
Transaction	The provision of any advice by a business or individual to a client by way of business, or the handling of the client's finances by way of business. A transaction could be simply operating across a client's account
Transaction Monitoring	Monitoring of customer transaction with towards money laundering and terrorist financing risks. Historical and current information and interactions of a customer is assessed within transaction monitoring
Transaction Screening	Customer screening that comprises transaction monitoring and enhanced transaction monitoring
UN	The United Nations
USA	The United States of America
Sum&Substance	AML Screening & Monitoring provider

INTRODUCTION

Document location

This document (AML and CTF) and other related documents can be found under policies and procedures on the company servers.

Introduction

This document describes FIATUM OÜ AML and CTF.

Document Purpose and Scope

To define accountabilities for the people, teams, or process that will be responsible in company business development.

Required Documentation

The conformance of actual procedures and practices to the documentation provided will be periodically checked by:

Henrich Lipskij	Director

This Policy, known as KNOW YOUR CUSTOMER (KYC) procedures and ANTI MONEY LAUNDERING (AML) measures approved by the Board. The policy is based on the approved guidelines issued by OECD and FATF.

The KYC guidelines have regularly been revised in the context of the recommendations made by the FATF and OECD on KYC, AML, CTF and other standards. These guidelines advise Financial Institutions (FI) to follow certain Customer Identification Procedure for opening of accounts and monitoring suspicious transactions in order to report to appropriate authority.

We approve a policy on Know Your Customers and Anti-Money Laundering measures including the above referred recommendations with the approval of the Board.

This manual is based on recommendations of OECD, FATF and Money Laundering Prevention Act for:

- Maintenance of Records of the Nature and Value of Transactions;
- Procedure and Manner of Maintaining and Time for Furnishing Information and Verification;
- Maintenance of Records of the Identity of the Customers of the FI and Financial Institutions.

This manual was written, considering the guidelines of the EU AML legislation, existing policy of the FI on KYC and AML and the business strategies of the FI.

MLRO contact details

Name: Henrich Lipskij

Phone number: +372 634 73 34

E-mail: director@fiatum.com

Any changes to this document must go through the same process as described above.

1. RISK ASSESSMENT

1.1 REGULATORY FRAMEWORKS

The legislation governing money laundering and terrorist financing and the fight against it is as follows:

1. Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA;
2. Directive 2018/843 (AMLD V) on anti-money laundering and terrorist financing (the Fifth Money Laundering Directive);
3. Money Laundering and Terrorist Financing Prevention Act 2017;
4. Anti-corruption Act 2012;
5. the Payment Institutions and E-money Institutions Act 2009;
6. the International Sanctions Act;
7. the Requirements and procedure for identification of persons and verification of person's identity data with information technology means 2018;
8. the Supervision policy of Finantsinspektsioon for countering money laundering and terrorist financing;
9. the Advisory Guidelines of Finantsinspektsioon "Organisational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing".

Fifth Money Laundering Directive

On 9 July 2018, the EU's Fifth Money Laundering Directive came into force.

Member States now have until 10 January 2020 to give effect in local law to its provisions, which impose a range of new requirements.

The amendments made by 5MLD form part of the EU Commission's action plan on further strengthening the fight against terrorist financing.

(i) 5MLD now amends 4MLD, increasing the scope of regulation in several significant ways, including in relation to the following key areas: custodian wallet providers and virtual currency exchange platforms added as new 'Obliged Entities'

(ii) tighter controls relating to KYC & EDD

(iii) tighter controls relating to transactions

(iv) tighter controls relating to high risk third countries

(v) access to information on beneficial ownership of corporates and trusts and also PEP lists through the centralised national registers.

- Virtual currency exchange platforms and custodian wallet providers.

As regards the Company's business, the key issue is the amendments in 5MLD bring custodian wallet providers i.e. cryptocurrency wallet services where the service holds its users' private keys.

and providers engaged in exchange services between virtual currencies and fiat currencies (i.e. platforms used to exchange money for cryptocurrency) within the scope of 4MLD.

This change is in order to address a risk that virtual currencies may be used by terrorist organisations to conceal financial transactions, as transfers with virtual currencies can be carried out anonymously.

- Lower limits in relation to CDD requirements on pre-paid instruments.

The threshold for a customer due diligence exemption for electronic money products, including prepaid cards, has been lowered from EUR 250 to EUR 150 for the maximum balance and maximum monthly transaction limit. There is a maximum limit of EUR 50 for redemption in cash, cash withdrawal of the monetary value or amount paid per remote payment transaction (for example, travel cards) above which limit the existing customer due diligence exemption will no longer applies.

- Clarifying EDD for high-risk third countries.

4MLD provides that once a country has been designated by the European Commission as having strategic money laundering or terrorist financing deficiencies, firms had to apply enhanced due diligence measures in respect to business relationships or transactions involving those countries.

5MLD sets out a prescriptive list of enhanced due diligence measures that Member States must require firms to apply for high-risk countries as defined by the European Commission.

These encompass checks on the client, note we shall only be dealing with individual clients at this stage, the source of funds and the monitoring of transactions. These are to be considered as a minimum set of requirements to be applied by all Member States. 5MLD also provides a non-exhaustive list of countermeasures that Member States and firms may apply when dealing with high risk third countries.

1.2 RISK BASED APPROACH AND CUSTOMER RISK GROUPS

Risk-based approach

FIATUM OÜ applies a "risk-based approach" to its customers. This approach includes the following consequent actions applied to each customer:

a) identifying money laundering and terrorist financing risks that a relevant to the customer's business;
b) carrying out risk assessment in the course of onboarding and periodically in the course of business relations, with the emphasis of the customer's behavior, delivery channels, patterns and irregularities;
c) designing and putting in place effective controls for the customer;
d) overseeing and monitoring the customer's practices, improving the established controls, where necessary;
e) maintaining records of risk assessment carried out.

Records of risk assessment must be approved by the MLRO. The MLRO has sufficient seniority and experience to approve the risk assessment of each customer.
FIATUM OÜ continuously reviews its implementation of risk-based approach based on best practices of applying risk-based approach, adopted in a public and private sector.

FIATUM OÜ does not provide its services to the companies, if their activity relates to the following:

- counterfeit goods / replicas;
- drug trafficking including chemicals used to manufacture synthetic drug or drugs;
- production or activities involving harmful or exploitative force on child labor;
- production, trade, storage, or transport of hazardous chemicals;
- any business relating to pornography or prostitution;
- abusing confidential or material, non-public information;

- trading of animal fur, bones and ivory;
- cultural objects like sculptures, statues, antiques, collectors' items, archeological pieces;
- production or trade in weapons and munitions;
- trading of Fireworks, explosives and Nuclear Weapons;
- human trafficking;
- human body parts and pathogens;
- bailiff services;
- jewel, gem, precious metal dealers without license;
- non-licensed counselling centers;
- timeshare, timeshare maintenance;
- pyramid selling;
- illegal telecommunication devices;
- non-licensed lawyer services and/or advice;
- non-licensed gambling;
- most-significant bit (MSB) activities;
- crowdfunding;
- fortune tellers, tarot card and horoscope readers, psychics;
- dating: subscription-based dating websites which do not have genuine, underlying matches or products;
- real estate / property clients: dealing in property that are not regulated by any AML regulations;
- trust and company service providers: their dealing is not regulated by any AML regulations.

Technological risk

Company also takes into account Technological risk factors when assessing risk and the extent of measures which should be taken to manage and mitigate that risk.

The Company's business model of receiving or paying cryptocurrencies, converting to fiat, and transmitting fiat funds to a merchant.

Our Risk Assessment of the Company's vulnerability to being utilised in any or all of these stages of money laundering is based upon a review how the business model targets client segments in each jurisdiction, our card issuing and Scheme Partner relationships, outsourcing arrangements especially of critical activities, volumes of transactions, how a client's use of our services develops as their relationship with the Company matures, and the basis on which we select cryptocurrencies to be made available for conversion into fiat; all these parameters may feature in determining on what basis the Company may be exposed to money-laundering.

However, the new technologies are also opening the way for the new types of monitoring. For example, the biometric face match and analysis of all parts of the blockchain in order to trace all illegal activities happened to the analyzed funds.

Customer risk groups

All customers of FIATUM OÜ are classified into three risk groups:

a) low risk customers;
b) customers who are of neither low risk nor high risk (medium risk customers);
c) high risk customers.

Criteria for the classification include:

a) customer risk factors, including whether:

(i) the business relationship is conducted in unusual circumstances;

(ii) the customer is resident in a geographical area of high risk (see sub-paragraph (c));

(iii) the customer is a legal person or legal arrangement that is a vehicle for holding personal assets;

(iv) the customer is a company that has nominee shareholders or shares in bearer form;

(v) the customer is a business that is cash intensive;

(vi) the corporate structure of the customer is unusual or excessively complex given the nature of the company's business;

b) product, service, transaction or delivery channel risk factors, including whether:

(i) the product involves private banking;

(ii) the product or transaction is one which might favour anonymity;

(iii) the situation involves non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

(iv) payments will be received from unknown or unassociated third parties;

(v) new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;

(vi) the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country;

c) geographical risk factors, including:

(i) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;

(ii) countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering, and the production and supply of illicit drugs;

(iii) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;

(iv) countries providing funding or support for terrorism;

(v) countries that have organisations operating within their territory which have been designated by countries governments, international organisations or the European Union as terrorist organisations;

(vi) countries identified by credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or non-governmental organisations as not implementing requirements to counter money laundering and terrorist financing that are consistent with the recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016.

Low risk customers

FIATUM OÜ uses its risk assessment in every case to determine the risk category for customers. Whilst easily identifiable customers may be indicative of lower risk, it must still consider the other relevant factors before a conclusion is drawn.

If a business relationship with, or transaction of the customer has been assessed to represent a low risk of money laundering, such customer should be deemed to be of low risk. Low risk customers are subject to simplified due diligence measures.

Low risk with full KYC documentation on file is subject to approval by MLRO on a case-by-case basis.

The following customers may be deemed to be of low risk:

a) public administration, or publicly owned enterprise;
b) a credit institution or a financial institution which is:

- subject to requirements in national legislation implementing the fourth money laundering directive as an obliged entity (within the meaning of that directive), and
- supervised for compliance with those requirements in accordance with section 2 of Chapter VI of the fourth money laundering directive;

c) a company whose securities are listed on a regulated market, and the location of the regulated market.

The following products, services, transactions or delivery channels may be deemed to be of low risk:

a) a life insurance policy for which the premium is low;
b) a financial product or service that provides appropriately defined and limited services to certain types of customers to increase access for financial inclusion purposes in an EEA state.

The following geographical factors (including where the customer is resident, established, registered or operates) may be deemed to be of low risk:

a) an EEA state;
b) a third country which identified as having a low level of corruption or other criminal activity, such as terrorism, money laundering and the production and supply of illicit drugs, and has effective regulatory frameworks, monitoring and enforcement systems, as mat be officially reported by the Financial Action Task Force, the International Monetary Fund, the World bank, the Organization of Economic Co-operation and Development, etc.

Low risk customers and their beneficial owners must be identified, and their identities must be verified.

Customers who are of neither low risk nor high risk (medium risk customers)

Customers who are of neither high risk nor low risk (medium risk customers) include those remaining beyond the joint scope of high risk and low risk customers. They are subject to:

- customer due diligence;
- transaction monitoring;
- full KYC procedures.

High risk customers

High risk customers include:

- legal formation, whose beneficial owner or representative is a PEP;
- those who is involved in business sector with high risk of corruption, or where cash transactions have an essential role;
- whose beneficial owner is a person involved in business sector with high risk of corruption, or where cash transactions have an essential role;
- those who, or whose beneficial ownership are related to any of the restricted countries listed in Appendix B “Restricted Countries” of this AML and TF Policy;

- those whose reason of establishment and (or) activities are unclear and the information on the legal and economic purpose of the customer's activity is general or limited, or is not available;
- is suspected to have such beneficial owner who is attempting to hide his or her identity by using family members or closely associated persons;
- whose previous activity and professional experience (previous activity and professional experience of its beneficial owner) is not related to the planned economic activity;
- whose economic activity, or whose beneficial owner's economic activity, does not correspond to the financial state of the customer (or such beneficial owner);
- those whose legal or economic grounds, or objective of business are unclear (for example, it is not possible to properly ascertain the movement of goods and services);
- in relation to whom any recipient bank of financial transactions sent requests;
- who is a financial institution, including a financial institution upon which sanctions are imposed as a result of violations of anti-money laundering and counter terrorist financing laws.

The above does not constitute an exhaustive list.

High risk customers are subject to enhanced due diligence, enhanced transaction monitoring and are obliged to prove their sources of funds. The listed procedures apply additionally to the procedures applied before, such as full KYC and CDD.

The degree of enhanced due diligence is determined by MLRO on a case-by-case basis.

Each customer is assessed in accordance with criteria and procedure set by sections 1.3 "AML: Risk Assessment Criteria" and 1.4 "Customer Risk Assessment Procedure" below.

Ongoing monitoring of customer identity

Ongoing monitoring of customer identity is done on a risk-based approach according to the frequency of the customer's risk assessment. This includes all information within the client file. FIATUM OÜ uses Sum&Substance for the ongoing monitoring.

1.3 AML RISK ASSESSMENT CRITERIA

ID	RISK DESCRIPTION	POTENTIAL OUTCOME
AML/R1	The customers are not who they say they are, the customer is not identified properly.	The PM does not know their customer. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R2	The customer provides incorrect address information.	The PM does not know their customer. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R3	The customer provides fraudulent or altered documents.	The PM does not know their customer. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.

AML/R4	PM is unable to verify customers.	The PM does not have the skills, experience or means to identify and verify the customer. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action. Failure to identify and report suspected money laundering. Failure to keep customer data up to date throughout the customer relationship. Failure to appropriately react to risk-based triggers.
AML/R5	Failure to keep customer data up to date throughout the customer relationship.	Failure to identify and report suspected money laundering. Failure to appropriately react to risk-based triggers.
AML/R6	Changes in a customer's circumstances are not monitored.	Failure to identify a dormant account reactivation and unauthorized use.
AML/R7	Customers are accepted from a jurisdiction which has not been approved for the product.	Potential breach of permission. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R8	The customer is a Politically Exposed Person (PEP).	The business does not identify where EDD should be completed. There is no process for dealing with a PEP should they be identified. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R9	The customer appears on one or more of the following Sanctions lists: • the UK HM Treasury sanctions list; • the US Office of Foreign Assets Control sanctions list, • the EU sanctions list (administered by the High Representative of the European Union for Foreign Affairs and Security Policy and the European Commission), • the UN sanctions list (administered by the United Nations Security Council). An existing customer becomes a sanctioned person during the course of relationship.	Having a customer who is on a sanctions list is in breach of the terrorist financing legislation. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action. The business does not identify where EDD should be completed.
AML/R10	The risk in dealing with someone on the sanctions list is that we are in	A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements

	breach of the terrorist financing legislation.	resulting in regulatory censure or legal action.
AML/R11	The PM does not have an effective process to analyze fuzzy matches.	A potential sanctions match is identified but not qualified or eliminated. The risk in dealing with someone on the sanctions list is that we are in breach of the terrorist financing legislation. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R12	The card is obtained by someone other than the customer.	The card has been obtained fraudulently. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R13	Multiple cards are provided to the same person (e.g. using different names but living at the same address).	The card has been obtained fraudulently. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R14	The customer has access to higher limits than required.	Increased exposure to financial crime and / or fraud activity related to money laundering. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R15	The customer has access to purse parameters / velocity limits which are not required.	Increased exposure to financial crime and / or fraud activity related to money laundering. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R16	Funds are received from a third party.	Money is received from an unverified 3rd party which is then laundered. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R17	We do not understand the Source of funds routinely loaded to the card.	Money is received from an unverified 3rd party which is then laundered. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R18	The source of the initial load is unknown and / or unusually high.	Increased exposure to financial crime and/or fraud activity related to money laundering. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R19	PM does not identify any unusual or suspicious activity on the card holder's account.	The product is used for fraud and/or money laundering purposes. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory

		censure or legal action.
AML/R20	Knowledge or suspicion of financial crime is identified but not reported.	A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R21	Cardholder is notified that a SAR has been submitted ('Tipping Off').	A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R22	Unauthorized persons attempt to access a customer's account.	Increased exposure to financial crime and/or fraud activity related to money laundering. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action
AML/R23	The customer loses their card and it is used by somebody else.	A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R24	The card is intercepted on route to the address provided during the onboarding stage.	The product is used for fraud and/or money laundering purposes. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R25	PM doesn't have enough resources to manage the product.	No one is looking at financial crime risk so there is a large financial, reputational and legal risk to the business due to the likelihood of this customer being involved in financial crime. A lack of or out of date AML/KYC/fraud procedures leads to a breach of legislative requirements resulting in regulatory censure or legal action.
AML/R26	Anti-Money Laundering/Financial Crime training is not or is inadequately provided.	Through lack of knowledge of procedures and legal requirements, staff act on client instructions without undertaking basic AML checks. This leads to unrecognized money laundering, resulting in criminal action including both financial penalty and custodial sentencing. Furthermore, there are potential reputational issues due to a lack of staff knowledge and the likelihood of being the victim of financial crime.
AML/R27	PM does not keep adequate records.	PM and Issuer in breach of record keeping requirements and unable to investigate and suspicion of fraud or financial crime properly.

1.4 CUSTOMER RISK ASSESSMENT PROCEDURE

The customer risk assessment scoring system represents by a numeric value the total money laundering and terrorist financing risk level of the Customer. The total number of points forms the overall risk profile of the customer (i.e. the customer's total MLTF risk, formed by the total risk enhancing factors associated with the client). FIATUM OÜ determines and maintains the scoring assigned to each risk factor (i.e. the assessment of the importance of the impact

of the risk factor which represents a numerical expression of the impact of the risk factor on the overall level of risk) and ensures it is automated application to determine the customer's risk level.

The total customer risk assessment scoring system score in the client's overall risk profile is 100 points. The above number of points in the customer risk assessment scoring system upon the assessment of the nature of company's economic activity and the client's MLTF risks is broken down by risk segments as follows:

- customer risk – 33 points;
- national and geographic risk – 20 points;
- risk-related to services and products used by the client – 27 points;
- service and product delivery channel risk – 20 points.

For each risk segment considered within the assessment, the risk score can never be zero. Whilst the risks within a factor can be extremely low, there is always an inherent money laundering and terrorist financing risk which needs to be acknowledged by FIATUM OÜ.

The monitoring employees ensure updates of the customer's risk profile by applying the customer risk assessment scoring system each time when it is required to carry out due diligence of the customer. The customer risk assessment scoring system is utilized to apply risk mitigation measures pursuant to this AML and TF Policy or when FIATUM OÜ has obtained (through IT reports, customer service or due diligence, mass media etc.) information concerning the customer, its beneficial owner, personal or economic activity as well.

The monitoring employee, based on the risk assessment and the risk profile of the customer (awarded score), determines the necessary due diligence measures and their regularity. The client's due diligence measures and their regularity is determined based on the existing level of risk.

At least once a year or more often (if necessary) if FIATUM OÜ obtains information which indicates changes in information on which the initial numerical score assigned to the risk factors was based, the company updates the numerical score.

In order to perform regular update of the numerical score assigned to the risk factor, the customer compliance and monitoring department head selects at least 10 (ten) clients (focus group) and the relevance of the numerical score assigned to each risk factor, as well as the necessary changes in the numerical score assigned to each risk factor is based on the monitoring of the activity of the focus group.

Before the implementation of a new customer risk assessment scoring system or significant changes to the existing client risk assessment scoring system, the company shall inform the commission in a written form.

The customer risk assessment scoring system shall include the following client identification information:

- name of the customer;
- country of registration of the customer;
- registration number of the customer;
- representatives of the customer;
- beneficial owners of the customer;
- online store website of the customer.

It is recognized that a higher level of due diligence and monitoring would be specified for business areas prone to higher money laundering and terrorist financing risks. Accordingly, entities, their owners, directors whose identities can be easily identified and transactions implemented by them and largely conform to the known profile, may be categorized as a low risk.

Further, customers that are likely to pose a higher-than-average risk to the FIATUM OÜ may be categorized as medium or high risk depending on factors such as merchant's backgrounds, nature and location of activity etc.

The risk assessment's scope includes, but is not limited to:

- the type, scale and complexity of the business;
- the products and services sold;
- target markets, high risk customers, jurisdiction exposure, distribution channels and transaction size;
- the volumes as compared to historic trends, systems, major organizational changes and compliance testing;
- the audit and regulatory findings.

The total numerical score assigned to the client in the client risk assessment scoring system shall be set according to the risk score indicated below regarding each of the following risk factors:

Customer risk form:

Risk enhancing factor	Risk score if YES	Risk score if NO
The legal entity with core activity in the EU.	1	0
The legal entity with core activity outside the EU but is a part of a publicly known foreign group with a good reputation.	2	0
The legal entity with core activity outside the EU and is not a part of a publicly known foreign group with a good reputation.	3	0
The legal formation, whose beneficial owner or representative is a PEP.	2	0
The legal entity recognized as a shell company.	3	0
The customer or the beneficial owner of the customer, or the representative of the client is an outsourced bookkeeper, lawyer or provides services for establishing and running legal entities who wish to conclude a contract with the company in his name to perform financial transactions on behalf of the client.	2	0
The activity of the client or the beneficial owner of the customer is related to: gambling; encashment; cash, currency exchange, marketing services; IT development, foreign exchange transactions, trading precious metals, weapons and other activity that is hard to document and trace.	3	0
The customer or the beneficial owner of the client is interested in the company's MLTF assessment policies and procedures or procedures that apply to PEP.	1	0
The customer or the BO of the client is a person related to the business sector with high risk of corruption.	2	0

The customer or the beneficial owner of the client is a person related to the business sector where cash transactions have an essential role.	2	0
The reason for the establishment of the legal entity is unclear and the information on the legal and economic purpose of the client's activity is general or limited or is not available.	2	0
It is suspected that the beneficial owner is attempting to hide their identity by using family members or closely associated persons.	2	0
The previous activity and professional experience of the client or the beneficial owner of the client is not related to the planned economic activity.	2	0
The economic activity does not correspond to the financial state of the client or the beneficial owner of the client.	2	0
The legal or economic grounds of the type of the customer's economic activity or transactions are unclear (for example, it is not possible to properly ascertain the movement of goods and services, the goods are sold outside the EU borders etc.).	2	0
Sum&Substance report received regarding the client indicates that the customer has high MLTF risk.	2	0

The maximum value of customer risk amounts to 33 points.

National and geographic risk form

Risk enhancing factor	Risk score if YES	Risk score if NO
The customer, the beneficial owner of the customer or the main cooperation partner is related to a country or a territory included in the cabinet list of low tax and duty-free countries and territories.	2	0
The customer, the beneficial owner of the customer or the main cooperation partner is related to a country or a territory associated with financial or civil restrictions imposed by the UN, the USA or the EU.	2	0
The customers, the beneficial owner of the customer or the main cooperation partner is related to a country or territory which is included in FATF list of "Non-Cooperative Countries or Territories" (NCCTs) or regarding which the FATF has issued a statement as a country or territory that has no laws and regulations for the money laundering and terrorist financing or where they have significant shortcomings and they do not meet international requirements.	2	0

The customer, the beneficial owner of the customer or the main cooperation partner is related to a country which is included in the list of states which have been identified as high money laundering and terrorist financing risk countries approved by the European Commission.	2	0
The customer, the beneficial owner of the customer or the main cooperation partner is related to a country where there are significant gaps in the area of money laundering and terrorist financing risk prevention.	2	0
The customer, the beneficial owner of the customer or the main cooperation partner is related to a country with a high level of crime that may result in money laundering.	3	0
The customer, the beneficial owner of the customer or the main cooperation partner is related to a country or a territory where there are no requirements to submit reports on the financial activities of the company or it is allowed to register a company without specifying the actual location.	2	0
The customer, the beneficial owner of the customer or the main cooperation partner is related to a country with a high risk of corruption.	2	0
The customer, the beneficial owner of the customer or the main cooperation partner is related to a country with an unstable political situation.	3	0

The maximum value of national and geographic risk amounts to 20 points.

Product/Services related risk form:

Risk enhancing factor	Risk score if YES	Risk score if NO
The customer requests options for anonymity and international use (e.g., online payments, prepaid cards, payment orders, payments made by phone and others) that provide an opportunity for large transactions (more than 100000 EUR per month) or large number of orders (more than 1000 per month).	3	0
The customer has been set/assigned an unusually large transaction limit or unlimited transactions.	3	0
The customer can carry out large, complex transactions (exceeding 100000 EUR per month) with a large number of parties (more than 3).	3	0
The customer has not participated in face-to-face identification.	3	0
The customer is found through agents without money laundering and terrorist financing risk prevention requirements or are not adequately monitored.	3	0

The provision of financial services is based on technological solutions which limits the identification of the customer and the information about the personal and economic activity (for example, video identification, e-commerce and its variations).	3	0

The maximum value of risk related to services and products used by the client amounts to 27 points.

Service and product delivery channel risk form:

Risk enhancing factor	Risk score if YES	Risk score if NO
Requests have been received from the recipient bank of the customer's financial transactions regarding the customer or the customer's transactions.	2	0
The customer is a payment institution and a monitoring institution has imposed sanctions on violations of anti-money laundering and counter terrorist financing requirements or faults.	2	0
The payment received or made significantly (10 percent of the set limit value) exceeds the limit value set by the company based on the results of the investigation of the client's economic activity.	2	0
The monthly credit turnover exceeds the equivalent of 300000 EUR or significantly exceeds other, lower threshold (10 percent of the limit value) set by FIATUM OÜ based on the results of the investigation of the customer's economic activity.	2	0
The three-month credit turnover exceeds the equivalent of 700000 EUR or significantly exceeds other, lower threshold (10 percent of the limit value) set by FIATUM OÜ based on the results of the investigation of the customer's economic activity.	2	0
The annual credit turnover exceeds the equivalent of 3000000 EUR or significantly exceeds other, lower threshold (10 percent of the limit value) set by FIATUM OÜ based on the results of the investigation of the customer's economic activity.	2	0
At least six months elapse between the date of the first transaction for the benefit of the customer and the date of establishing the business relationship with the customer, and the monthly credit turnover has reached the equivalent of 70000 EUR.	2	0
The average number of operations per month exceeds 1000 EUR.	2	0
The average amount per operation exceeds 500 EUR.	2	0
The customer is an association or foundation and during	2	0

the business relationship money is transferred abroad and the amount of the transaction exceeds the equivalent of 10000 EUR.		

The maximum value of service and product delivery channel risk amounts to 20 points.

The customer risk assessment scoring system shall include the following information:

- the customer's initial assessment date, name and surname of the employee who performed the risk assessment, as well as the resulting customer risk score;
- the date of each further customer's assessment, name and surname of the employee who performed the risk assessment, as well as the resulting customer risk score.

Each assessment score shall be recorded in the customer risk assessment scoring system, as well as printed and signed by the employee who performed the risk assessment and added to the customer's file.

Before establishing business relationship, the monitoring employee, upon receiving the potential customer's risk score in the customer risk assessment scoring system, should:

- print out the customer risk assessment scoring system score summary regarding the potential customer, sign it and include it in the potential customer's case;
- record the information about the potential customer's risk score in the company system and the monitoring employee statement on the customer;
- if according to the result generated by the customer risk assessment scoring system the customer due diligence is required upon establishing business relationship, the employee shall carry out customer due diligence in addition to the initial customer assessment procedure pursuant to the client compliance procedure regulations;
- a written statement is drawn pursuant to the customer compliance procedure with a proposal for the draft decision regarding establishing business relationship with the potential customer pursuant and submitted to the customer compliance and monitoring department head.

During the business relationship, the monitoring employee, upon receiving the potential customer's risk score in the customer risk assessment scoring system, should:

- print out the customer risk assessment scoring system score summary regarding the customer, sign it and include it in the customer's case;
- record the information about the customer's risk score in the company system and the customer monitoring employee statement on the customer's activity;
- if according to the result generated by the customer risk assessment scoring system a customer's due diligence is required upon establishing business relationship, the employee shall carry out customer's due diligence in addition to the initial client assessment procedure pursuant to the customer compliance procedure regulations;
- a written statement is drawn pursuant to the customer compliance procedure with a proposal for the draft decision regarding continuation or termination of the business relationship with the potential customer and submitted to the client compliance and monitoring department head.

The monitoring employee, in regard to each customer, shall monitor whether the risk score assigned to the customer is effective and complies with the management of the relevant risks. Having found gaps or inconsistencies in the customer risk assessment scoring system the client monitoring employee shall immediately

notify the head of customer compliance and monitoring department and the member of the board of the company responsible for money laundering and terrorist financing risk prevention.

FIATUM OÜ shall terminate the business relationship with the customer if within 30 days after the preconditions for due diligence have been established the minimum requirements for customer due diligence cannot be met and there is no sufficient evidence to provide the legal and economic purpose of the customer's transactions.

The customer's risk score assigned in customer risk assessment scoring system upon making the decision on the cooperation with the potential client or the cooperation with the existing client and:

- if the customer's risk score in the section "customer risk" is at least 8 - the customer is assigned a high-risk customer status and due diligence is applied before establishing cooperation;
- if the customer's risk score in the sub-section "National and geographical risk" is at least 4 - the customer is assigned a high-risk client status and due diligence is applied before establishing cooperation and during the cooperation;
- if the customer's risk score in the section "risk related to services and products used by the customer" is at least 3 - the client is assigned a high-risk customer status and due diligence is applied before and during the cooperation;
- if the customer's total risk score is at least 10 - the client is assigned a high-risk customer status and due diligence is applied before establishing cooperation and during the cooperation;
- if the customer's total risk score is at least 10 - the client is assigned a high-risk customer status and due diligence is applied before establishing cooperation and during the cooperation;
- if the client's total risk score is at least 15 - the customer is assigned a high-risk customer status and due diligence is applied, as well as increased monitoring of transactions is carried out by setting one or more limitations set out in the customer compliance procedure;
- if the customer's total risk score is at least 20 - A decision is made not to establish (refuse) cooperation (business relationship) with the potential client or to terminate the cooperation (business relationship) with the existing customer.

2. RISK MITIGATION MEASURES

2.1 CUSTOMER RISK MITIGATION PROCEDURE

FIATUM OÜ understands that the Risk Assessment starts during the underwriting stage. That is why customer screenings are implemented in order to spot any potential threat to our business operations and to our reputation.

FIATUM OÜ partners with world`s first-class risk prevention and mitigation services enhances customer checks by doing the following:

- customer screening before boarding: a comprehensive background report is provided, which allows us to know who we're dealing with before signing the contract. It also reduces the time needed to conduct due diligence of customer;
- simple and regular customer monitoring: it provides automatic follow ups on our current customers online activities;
- constant long-term protection: the software protects our reputation by reducing the risk of falling victim of a fraudulent customer.

Also, during the underwriting stage, the customer is provided with general and specific processing rules which serve as guidelines for future partnership with FIATUM OÜ. Among other things, such rules aim to anticipate and reduce the threats associated with each type of customer.

This is applicable to B2B customers and mostly for those who sell goods or services online.

AML risk mitigation procedure:

The usage of internet online research tools and sources below has a significant role in AML risk mitigation process when speaking about the business customer.

1. who is Information on the website (especially for online business);
2. scoring systems usage like Alexa;
3. Website PageRank like Google;
4. social bookmarks;
5. wayback machine;
6. reverse-IP analysis;
7. text analysis;
8. source code analysis;
9. comparing products with competitors' websites;
10. extensive internet research;
11. corporate data collection sites;
12. online complaints boards;
13. reverse image search;
14. Google analytics;
15. TOR-browser and proxy server.

2.2 CUSTOMER DUE DILIGENCE

FIATUM OÜ applies Due Diligence at the start of customer engagement by identifying and verifying customer identity on the basis of documents, data or information obtained from a reliable and independent source.

FIATUM OÜ conducts CDD both for natural customers, business customers, merchants and cardholders as detailed below.

FIATUM OÜ identifies the beneficial owner of the customer (for both legal entities and individuals) and takes adequate measures, on a risk sensitive basis to verify his identity (including in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure).

FIATUM OÜ creates policies and procedures that relate to customer due diligence, ongoing monitoring, and suspicious transaction reporting and record keeping.

If any suspicions are identified, these should be raised to the MLRO for further investigation by completing the relevant internal suspicious activity report (SAR) form.

The purpose of the customer due diligence (CDD) process is to collect, process, verify and keep the information about FIATUM OÜ customers, in order to minimize the possible and potential ML/TF risks. There are circumstances in which enhanced due diligence should be applied and those in which simplified due diligence may be appropriate:

- it should be recognised that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases in which particularly rigorous customer identification and verification procedures are required;
- the relationships with individuals who hold or have held important public functions within the European Union or internationally and particularly individuals from countries where corruption is widespread.

Since FIATUM OÜ deals with customers whose residences are often outside of the Republic of Estonia, all foreign language documents received as a part of customer due diligence that are not in Estonian or English language must be translated by a professional into English.

FIATUM OÜ uses a minimal allowed limit of 150 EUR to those customers who have opened an account with minimum requirements. The specified turnover limit is applied separately to sending and receiving transactions, and the verification requirement applied when either of the two are exceeded.

In respect of products benefiting from due diligence, identity must be verified before cumulative turnover limits are exceeded. Therefore, the systems are in place to anticipate the approach of limits and to seek identification evidence in good time before the annual turnover limits are reached. The customer's account must be frozen if the limits are reached before the verification of identity has been completed.

FIATUM OÜ applies customer due diligence measures when:

- the customer establishes a business relationship;
- the customer carries out an occasional transaction that amounts to a transfer the funds transfer regulation exceeding 1000 euros (or the equivalent in another currency (including cryptocurrency));
- there is reasonable ground for suspecting money laundering or terrorist financing;
- there are any doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

When the customer is not a high value dealer or a casino, FIATUM OÜ must also apply customer due diligence measures if such relevant person (the Firm) carries out an occasional transaction that amounts to 15000 EUR (or the equivalent in another currency (including cryptocurrency)) or more, whether the transaction is executed in a single operation or in several operations, which appear to be linked.

2.3 CUSTOMER IDENTIFICATION

Customer identification is an essential element of 'know your customer' (KYC) standards. Current KYC forms are available electronically on the FIATUM OÜ website (https://fiatum.com/) after a client's registration of its personal account.

Whether the customer is a business or individual, the customer should be identified in the risk assessment and with standard due diligence procedure implemented by the Firm.

FIATUM OÜ maintains a systematic procedure for identifying new customers and cannot enter into a service relationship until the identity of a new customer is successfully verified.

For customers who do not provide the relevant KYC documentation for CDD purposes, the Firm must access the reasons why and, where appropriate, consider raising a SAR.

Procedures document and enforce policies for identification of customers and those acting on their behalf. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. FIATUM OÜ pays special attention in the case of non-resident customers and in no case, short-circuit identity procedure is followed just because the new customer is unable to present enough documents and information to satisfy the KYC and due diligence procedures followed.

FIATUM OÜ can be exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. In each case reputational risk may arise if FIATUM OÜ does not diligently follow established KYC procedures. Particular safeguards have been put in place internally to protect confidentiality of customers and their business, FIATUM OÜ ensures that equivalent scrutiny and monitoring of these customers and their business is conducted, e.g. it is available to be reviewed by Compliance Officer.

FIATUM OÜ must identify its customer unless the identity of that customer is already known to and has been verified by the relevant person. After the customer has been identified, FIATUM OÜ must verify the customer's identity unless the customer's identity has already been verified by the relevant person. Amount of information to be received from a customer depends on whether the customer is a legal entity or an individual (natural person), namely:

- if a customer is legal entity, then at least the following information must be received for identification purposes: company name, registration number, address of the registered office (and, if different, its principal place of business), the law to which the legal person is subject to, its constitution (whether set out in its articles of association or other governing documents), full names of the board of directors (or if there is no board, the members of the equivalent management body) and the senior persons responsible for the operations of the legal entity;
- if a customer is an individual (natural person), then at least the following information must be received for identification purposes: name and surname, personal identity number (if such exists), date of birth, photograph on an official document which confirms his/her identity, residential address, number and date of issue of the personal identification document, state and authority which has issued the document, period of validity for identification document.

Customers who refuse to provide information:

Risk-based approach lies at the very foundation of FIATUM OÜ AML program. The rule that FIATUM OÜ considers as one of the most important is to KYC in order to minimise all possible risks connected with unknown identity of natural customers, business customers, merchants as well as cardholders which can be caused by lack of verification and unusual merchant`s or cardholder`s behaviour. It could be detected during ongoing transactions monitoring.

In a case where a potential merchant refuses to provide required information, FIATUM OÜ would not establish any business relationship with this merchant. If FIATUM OÜ reveals the fact that cardholder who implements large amounts of transactions does not want to provide the information needed for establishing his/her identity FIATUM OÜ would not approve the transactions and further transactions made by this cardholder, unless he provides all required documents.

Customers – insufficient or suspicious information:

- provides unusual or suspicious identification documents that cannot be verified;
- reluctant to provide complete information about the nature and purpose of business;
- the background is questionable or differs from expectations based on business activities;
- the customer has no discernible reason for using the company`s service.

FIATUM OÜ scrutinizes transaction flow throughout the course of any business relationship to ensure consistency with the knowledge of customers, their business and risk profile.

The MLRO conducts ongoing monitoring of all high-risk activity including customers who regularly implement large amount of transactions.

FIATUM OÜ collects the following information for identification purposes respectively for legal entities and natural persons:

For natural persons (beneficiaries and authorities)	
At a minimum	**Potential additional information (on the basis of risks)**
Legal name (first names and last name)	Any other names used (such as marital name, former legal name or alias)
Complete permanent address, whenever applicable	Professional address, post office box number, e-mail address and landline or mobile telephone numbers
Nationality, an official personal identification number or other unique identifier	Resident status
Date and place of birth	
For legal entities	
At a minimum	**Potential additional information (on the basis of risks)**
Name, legal form, status and proof of incorporation of the legal entity	
Permanent address of principal place of the legal entity's activities	
Official identification number (company registration number, tax identification number)	Legal entity identifier (LEI) if available
Mailing and registered address of legal entity	Contact telephone and fax numbers
Identity of natural persons who have authority to operate the account and who exercise control of the	Identity of relevant persons holding senior

legal entity through ownership or other means	management positions.
Identity of the beneficial owners	
Powers that regulate and bind the legal entity	

List of acceptable identification:

- current passport;
- current national identity card;
- travel documents;
- current EU residence permit;
- current full EU driving license;
- EU parking card for people with disabilities;
- the European Health Insurance Card.

List of acceptable address verification:

- utility bill (dated within the past 6 months);
- telephone bill (dated within the past 6 months) – mobile phone bills are not acceptable;
- sky or cable TV bills (dated within the past 6 months);
- credit card bill (dated within the past 6 months);
- certain conditions may apply for overseas financial providers;
- bank, building society, credit union statement – showing current activity (dated within the past 6 months);
- certain conditions may apply for overseas financial providers. The mortgage statement from a recognized lender (dated within the past 12 months);
- home office letter confirming right to work in the EU (dated within the past 6 months);
- EU parking card for people with disabilities;
- the current motor insurance certificate/schedule (a cover note is not acceptable);
- the tenancy agreement (must be from a local council or reputable letting agency);
- the European Health Insurance Card.

Non-UN residents:

- due to the new legislation non-EU residents must always present their passport or national identity card when applying for an account.

FIATUM OÜ may request information on the customer's beneficial ownership exercised through indirect shareholding by sending notices.

Obtaining information to identify the customer if it is a legal entity:

Our document requirements comply and often surpass the standard requirements:

- FIATUM OÜ forms;
- corporate documents:

1. certificate of incorporation;

2. incorporation documents showing directors and shareholders (not only company representatives, we perform full UBO identification, in case of more complex structures, we collect information about all owning companies).

- passport/national ID(s) of directors and shareholders owning more than 2% company shares (we do accept companies created with hosts);
- bank statements as a proof of accomplished bank's verification procedures (recent 3-6 months);
- processing statements (recent 3-6 months);
- company utility bills;
- re-presentment files;
- domain ownership.

FIATUM OÜ forms include:

- pre-application form – containing basic information, useful while presenting a customer;
- preliminary scan form - a substitution (along with forecast) for the pre-application. Contains basic company data required to start automated reputational checks;
- contact form – 8 key contacts, strategic from the point of view of business development;
- bank details form;
- forecast form– ongoing four-month processing prognosis, part of the agreement;
- transaction limits or recurring billing form.

Verifying the customer and/or beneficial owner(s) identification information:

In some cases, the customer's information is obtained directly from the customer. In other situations, the information is obtained from other sources. Irrespective of how or where the identification information is obtained, a determination must be made whether the information also needs to be verified.

Irregularities in the above documentations may be indicators for suspicion, leading underwriters and risk staffs to do additional research.

KYB optional documents

For some specific customers' applications (related to higher risk or for merchants providing services that may be regulated by some authorities) FIATUM OÜ might request some more specific documents:

- resume or CV(s) of directors and owners and detailed business plans with 6-month prognosis (if processing history not available);
- annual tax documents (for company and director or shareholder);
- business / operating licenses and permits;
- legal opinions - in case of any doubts about the customer's business if it is legal in the incorporation country;
- Certificate of Good Standing issued by competent authorities (issued for example by states secretaries);
- list of businesses that Company principals and/or beneficial owners own(ed)/operated) or have been involved in the past 5 years (statement).

Apart from additional documents in some cases collaterals could be implemented and have to be properly calculated (for example in case of long breaks between payment and fulfilment, i.e. Travel agencies).

Website compliance check

FIATUM OÜ implements checks of customers' websites that must comply with the following requirements. Every website that is about to be used for ecommerce processing must comply with the specific requirements regulated by card schemes (Visa/MC, Union):

- clear posting of the Refund and Return Policy;
- clear Privacy Policy;
- clear statement on website regarding security controls used to protect customers;
- clear posting of the Terms and Conditions;
- clear posting of the customer service telephone number and email address;
- clear posting of delivery methods and delivery times (if applicable);
- clear posting of the company legal name and corporate address;
- clear posting of the billing descriptor on the payment page;
- card Schemes logos visible on the payment page.

Contact information and customer support are always verified by performing test calls/emails.

Conducting customer screening

FIATUM OÜ understands that the risk assessment starts during the underwriting stage. That is why screenings are implemented in order to spot any potential threat to our business operations and to our reputation.

Reputation should be handled in two ways - manual and automatic/semi-automatic. For manual checks the key tool is the web search engine (i.e. Google, Bing, Yahoo) along with some more specific tools like who.is (for domain information), robtex.com (for domain and IP related checks) and alexa.com (to estimate the website traffic).

During manual check some key data like customer/merchant name, directors' names, URL address and related phones, emails and addresses should be checked along with phrases that may occur in regard to the business model (i.e. crime, scam, review) to narrow search results to the results really interesting in terms of international investigation (i.e. if merchant's director is a felon or a convict or known fraudster).

Generally, in case of suspicious customers/merchants usually director's full name or merchant's company name should return some results that will give the initial information to follow up or reject application at the early stage, however that is not a rule and sometimes the important results are found in most unexpected places.

Automated check

Parallel to manual screening FIATUM OÜ screens its customers with the use of Sum&Substance. This verification services provider allows to achieve high accurateness of verification through the automated check system. Sum&Substance provides FIATUM OÜ with the following services:

- email verification;
- phone verification;
- identity document verification;
- automated data extraction (basic five fields and additional fields);
- liveness check and face match;
- known face search;
- AML Screening, International Sanctions, PEPs, Watchlists and Adverse Media;
- Proof of address check;

- Ongoing document monitoring;
- Ongoing AML monitoring etc.

2.3.1 REMOTE CUSTOMER IDENTIFICATION RULES

Remote customer identification will be possible in one of the following ways:

- when information about a person's identity is certified by a qualified electronic signature which complies with the requirements of Regulation (EU) No 910/2017;
- when information about a person's identity is confirmed by electronic identification means issued in the European Union and functioning under electronic identification schemes with high or substantial assurance level under Regulation (EU) No 910/2017;
- using electronic means, allowing direct view transmission, in one of the following ways:
  1. identity document or residence permit in European Union captured using video-streaming and identity confirmation using at least an advanced electronic signature, meeting the requirements of Regulation (EU) No 910/2017,
  2. customer's facial image and original identity document captured using video-streaming.

Transmitting both videos and photographs using above mentioned means will be allowed. There is a requirement for video-streaming to be direct and live, which means that videos or photos not taken during live video-streaming will not be accepted.

With this function the company would verify its customers' identity in a few minutes – easy, secure and in compliance with the law. It would use an EU-certified or EU-patented solution. All the customer needs are:

- an internet access;
- a computer with webcam or smartphone or tablet;
- valid identity document.

It enables identification by video chat or photo whilst taking into account all the requirements set forth in the Money Laundering Act, data protection directives and the requirements laid down by the respective supervisory authorities (e.g. BaFin, FIAU, FINMA or FMA).

The company is planning to use one of the following or both remote customer identification method to open an account for the customers:

- live video streaming or photo identification.

Requirements:

- Internet access;
- computer with webcam, smartphone, table;
- valid identity document Account opening process;
- choose account type;
- customer fills out application form;
- scan requested documents and upload;
- customer introduces itself;
- confirms email address;
- confirms phone number;

- pairs his device;
- enters identification code Send by SMS or email;
- starts 5-minute video verification.

What data are collected:

- client-ID;
- name;
- street;
- ZIP/City;
- country;
- e-mail;
- mobile;
- ID-Card (passport);
- birthday;
- nationality.

What type of information is verified:

- ID Data verification;
- video conference verification;
- hologram verification;
- biometric recognition;
- TAN Code verification;
- PEP Scan verification;
- sanction list verification;
- e-mail verification;
- address verification.

Data transfer:

Scan all customer documents we receive, including personal identification (passport or driving license), proof of address (a recent electric bill) or credit cards are uploaded via a secured API or an embedded frame, or send them in an encrypted email to the verification partner – 3rd party certified vendor.

Additional verification that might be applied:

- cross-checked with location;
- identity;
- residence;
- IP address;
- GEO-IP location;
- internal blacklist.

Remote identification comes only as an initial KYC/CDD process to get into relationships with the customer. All other procedures apply in addition to this process if it would be required by the company policy, limits or law.

Where the customer refuses, or fails to provide FIATUM OÜ for the required documents and information for identification and creation of economic portrait, before entering into the business relationship, or during the execution of an individual transaction without adequate justification FIATUM OÜ will not proceed in a contractual relationship or will not execute the transaction and may also report it to AML officer. This can lead to a suspicion that the client is engaged in money laundering and terrorist financing.

If during the business relationship the client refuses or fails to submit all required documents and information, within reasonable time, FIATUM OÜ has the right to terminate the business relationship and close the accounts of the client. The compliance department also examines whether to report the case to AML officer.

2.3.2 REMOTE IDENTIFICATION LOGICAL PROCESS EXAMPLE

The steps below guide to complete and successfully remote identification:

1. **Identity document:**

The customer can provide passport, ID card, or driving license as an ID document. Please, fill in data on your ID using the characters of Latin alphabet as shown on example below:

- issuing country;
- identity document serial number;
- document issue date;
- gender;
- first name;
- last name;
- date of birth;
- place of birth.

2. **Personal information:**

In this step, the customer enters information in respective fields. The customer must make sure the data is correct and filled in English language.

3. **Addresses**:

The customer fills in up-to-date information regarding residential (current) address and permanent address. If the customer`s residential (current) address matches the customer`s permanent address, the customer can check "Same as residential". The customer should keep in mind that the permanent address should be the same as the billing address used for official correspondence.

4. **Scans of documents:**

The customer uploads photos/scans of document supporting information provided during the previous steps. The customer makes sure that its photos/scans meet the following requirements:

- documents should be valid;
- photos/scans of both sides of documents should be uploaded;
- scanned images should be in color and in high resolution (at least 300 dpi);
- allowed formats: JPG, GIF, PNG, TIFF or PDF;
- file size should be no more than 15 MB;
- photos/scans should not be older than 3 months;

- documents should be issued using characters of Latin alphabet or have Latin transliteration of main fields.

5. **Identity documents:**

The customer must provide photos/scans of the identity document that was used to fill in the Verification form. Choose one of the following options:

- national ID card (both sides) or national passport (reversal);
- international passport (reversal);
- driving license (both sides).

FIATUM OÜ accepts a driving license as a proof of your identity only if it is a plastic card and all the information is provided with Latin transliteration.

6. **Selfie/video with identity document:**

The customer should make a selfie/video while holding an identity document that was used to fill in the verification form.

Before uploading an image on the verification form, customer must make sure to follow these photo/video requirements:

- he or she is looking straight at the camera;
- his or her background has a light, neutral color;
- his or her selfie/video is in color;
- no red eye;
- the customer does not wear sunglasses, a hat or a headband;
- information on the document must be clearly visible.

7. **Proof of residency:**

The customer must provide photos/scans of documents proving the address stated in the Verification form. Choose one of the following options:

- utility bill (NOT mobile phone, satellite/cable TV or printed Internet bills);
- electricity bill;
- bank statement;
- tax return, council tax;
- other documents, with the exception of electronic bills/statements, online screenshots, mobile phone bills or credit card statements.

8. **Documents upload:**

- documents should be valid (issued within the past 4 months);
- proof of residency document is addressed to the customer;
- proof of residency document is addressed to a home address (not a P.O. Box or any sided address);
- proof of residency document must be a photo or scanned image of a PAPER document;
- documents should be issued using characters of the Latin alphabet;
- proof of residency document must contain date of issue.

9. **The customer starts the verification process.**

2.3.3 SIMPLIFIED DUE DILIGENCE (SDD)

Simplified due diligence means not applying all measures of standard customer due diligence. It is, however, still necessary to conduct on-going monitoring of the business relationship. FIATUM OÜ must have reasonable grounds for believing that the customer, transaction or product relating to such transaction falls within one of the categories set out and may have to demonstrate this to their supervisory authority.

SDD triggers

Usually, if the client is a well-known public authority, listed on a regulated market or their transaction is below a certain amount, to remove unnecessary friction, they are exempt from tougher CDD checks.

Prior to applying SDD, FIATUM OÜ will conduct and document appropriate testing to satisfy itself that the customer qualifies for the simplified treatment under this policy and applicable legislation.

If at any point during relationship with the customer additional information, which suggests that the customer or service may pose a higher risk than originally expected, becomes available, standard or enhanced due diligence shall be conducted according to established risk profile of the customer.

SDD measures

Unlike in standard or enhanced due diligence, SDD does not require verifying a customer's identity.

Clearly, for operating purpose FIATUM OÜ will nevertheless need to maintain a base of information about the customer. FIATUM OÜ may apply a 'lighter touch' in terms of the extent of CDD undertaken.

Also, under SDD, the Firm might omit sanctions and PEP's screening procedure if a customer is categorized as a low-risk.

2.3.4 ENHANCED DUE DILIGENCE (EDD)

FIATUM OÜ conducts enhanced due diligence in the following cases:

- there is reasonable suspicion that the customer is a shell bank or a credit or a financial institution which is known to allow its account to be used by a shell bank;
- the customer's beneficial owner is a politically exposed person (PEP), or whose beneficial owner is a family member of PEP or the person known to be close associate of PEP, or is suspected to be any of such persons;
- the customer is classified as a high-risk customer, or suspected to be of high risk;
- the customer's beneficial owner is suspected to be related in any of the restricted countries specified in Appendix B "Restricted Countries" of this AML and TF Policy;
- the customer or its beneficial owner is involved in a business sector with a high risk of corruption, or where cash transactions have an essential role, such as forex trading, adult – related activities, unlicensed pharmaceutical, metallurgy, etc.

The scope of enhanced due diligence includes the following:

- obtaining additional information on the customer and on the customer's beneficial owner;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;
- obtaining information on the reasons for the transactions;

- obtaining the approval of senior management for establishing or continuing the business relationship;
- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

FIATUM OÜ increases the degree and nature of monitoring, in order to determine whether those transactions or activities appear suspicious.

In addition to the actions reflecting the minimum scope of enhanced due diligence, FIATUM OÜ may perform identification of the source of funds, by requesting the customer's declaration on its origin of funds, analyzing its tax filings, and transactions documents.

The degree of enhanced due diligence is determined by MLRO on a case-by-case basis.

2.3.5 REGULAR CUSTOMERS/CARDHOLDERS FULL DUE DILIGENCE

FIATUM OÜ follows reasonable procedures to verify and identify customers/cardholders who make transactions for large amounts (customers/cardholder due diligence). Such procedure of identification and verification of customers/cardholders based on information the firm collects from the customers/cardholder and then this information is verified.

FIATUM OÜ risk department, first of all, collects certain customer identification information from each customer who implements transaction for large amount, secondly, utilizes risk-based measures to verify the identity of every customers/cardholders who implements transaction for large amount, thirdly, records customer identification information and the verification methods and results, finally, using gathered information about the cardholder, risk department makes cardholder screening against OFAC and other sanction lists.

For all customers CDD must be completed prior enter into the relationship and it is necessary to complete the steps as follows:

- perform identification and verification – identify and where required verify the identity of the prospective customer and related parties;
- screen all customers and related parties against the EU sanction list, OFAC list, UN list;
- screen all customers and related parties to determine if there are any PEPs associated with the customer, by using public, trustable and opened information source;
- determine customer risk rating;
- complete EDD as required by the risk rating.

Minimum information to create customer's file:

Natural persons:

- name, surname;
- original and current identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as passport, national identification card or alien identification card with date of birth and place of birth;
- living address and postal code;
- officially certified copies of the above documents;
- disclaimer/questionnaire for the origin of funds not being derived from the proceeds of crime.

Legal entities:

- company' name;
- beneficial owner name;
- ownership memorandum, article of association etc.;
- legal and physical address;
- other relevant documentation such as company's activity details, expected turnover etc.;
- officially certified copies of the above documents;
- expected type and volume of transaction;
- main counterparties and countries;
- disclaimer/questionnaire for the origin of funds not being derived from the proceeds of crime.

FIATUM OÜ requirements for the customers/cardholders who exceed certain thresholds include following documents:

- a signed Authorization Form (form must be as provided by FIATUM OÜ or approved by the Risk and Compliance Department if furnished by the Merchant);
- a copy of a valid government issued ID with photo;
- a copy of the Credit or Debit card(s) listed on the Authorization form, both front and back with digits 7 through 12 (from the left) of the card covered or masked, the expiration date covered or masked;
- a copy of a recent utility bill or a bank statement displaying the home address as stated in the Authorization Form.

In verifying the information, FIATUM OÜ will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth allows us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- for an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- for a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

2.3.6 DEBIT CARDS PROCEDURES AND POLICIES

FIATUM OÜ is engaged in issuing online cards. Appropriate compliance with all KYC/AML/CFT guidelines issued periodically, in respect of add-on/ supplementary cardholders also shall be ensured.

Prepaid Cards shall be given to customers on submission of a respective Form duly filled and signed by the customer. KYC verification must be fulfilled for the cards on the basis of the form, submitted by the customer.

FIATUM OÜ must be rest assured that appropriate KYC procedures are efficiently managed and fulfilled before issuing debit cards to the clients sourced through agents (if any), and that the agents are also subject to KYC policies.

2.3.7 IDENTIFICATION OF BENEFICIAL OWNERSHIP

General

FIATUM OÜ analyses the entire ownership chain of each customer who is a body corporate. Such ownership chains may include persons with significant control, who may be represented by legal entities, individuals, trusts and firms.

FIATUM OÜ keeps records of actions taken in order to identify the beneficial ownership.

In each case, FIATUM OÜ determines the nature and extent of the beneficial interest is held.

The documents specified in this section are additional to the documents collected by FIATUM OÜ in the course of due diligence. The data obtained from the documents should be compared and analyzed comprehensively.

Procedure

FIATUM OÜ takes all reasonable steps to identify beneficial owners and control structure of each customer. When the customer is a part of a group, beneficial ownership and control chain within the entire group is subject to identification. FIATUM OÜ exhausts all possible means to perform, unless:

- there are no grounds for suspicion that no beneficial owner is identified;
- there is no any doubt that each natural person identified is a beneficial owner, and all beneficial owners are known to FIATUM OÜ.

The scope of analysis under this section should be as follows:

- control and ownership structure of the customer;
- relationships that a controlling person has with the customer's governing bodies and directors;
- ownership of the customer's assets and agreements in accordance with which such assets are held by its owners;
- the provisions of the customer's constitution on shares, the rights attached to them (including veto rights), profit sharing;
- the number of shares or securities which the shareholders hold;
- shareholders' investment, trust and other agreements which may change allocation of voting rights.

To identify beneficial ownership of a customer, FIATUM OÜ relies on the following evidence:

- the customer's documents and records in relation to its shareholders, beneficial owners and directors;
- the data of central public registers (including those held in European e-Justice Portal, the European Business Register, registers held by competent authorities of certain European countries) concerning shareholders of the legal entity, as well as its directors;
- trust agreements, shareholders' agreements (including voting agreements), agreements with the customer's creditors (including investors) and shareholders under which that may participate in corporate governance;
- agreements establishing a foundation or legal arrangement similar to trust;
- the customer's constitutional documents concerning shares, voting rights, shareholding benefits, management;
- written declaration of the customer of its beneficial ownership;
- agreements establishing a foundation or legal arrangement similar to trust.

The following information should be found in relation to each beneficial owner:

- name;
- month and year of birth;
- nationality;
- the country of residence;
- the date when the person gained beneficial ownership over to the customer;
- which conditions for being a beneficial ownership are met.

Circumstances which are indicative of beneficial ownership

In addition to cases when beneficial ownership is obvious, FIATUM OÜ may examine the customer against common scenarios where a person exercises control over business. The scenarios demonstrate, what precisely may constitute a beneficial ownership. They include the following.

1) A person has absolute decision rights or veto rights related to the running of the customer's business, for example:

- adopting or amending the customer's business plan;
- changing the nature of the customer's business;
- making any additional borrowing from lenders;
- establishing or amending any profit-sharing, share option, bonus or other incentive scheme of any nature for directors and employees.

2) However, if a person holds absolute veto rights for the purposes of protecting minority interests in the entity then this is unlikely, on its own, to constitute control over the customer. When used for the purposes of protecting minority interests these veto rights could include:

- changing the customer's constitution;
- duration of shares or rights;
- making any additional borrowing from lenders, outside previously agreed lending thresholds;
- winding up the entity.

3) Where a person holds absolute veto rights over the appointment of majority of directors.

4) A person shall not be deemed having beneficial ownership where the absolute decision rights or veto derive solely from being a prospective vendor or purchaser in relation to the entity, for a temporary period of time.

5) A person has the right to exercise beneficial ownership over a trust or firm if that person has the right to direct or influence the running of the activities of such trust or firm. For example:

- an absolute power to appoint or remove any of the trustees, except through application to the courts;
- a right to direct the distribution of funds or assets;
- a right to direct investment decisions of the trust;
- a power to amend the trust deed;
- a power to revoke the trust.

Such person may be the trustee, settlor, beneficiary or other person who is actively involved in directing activities of the trust.

6) In the case of a firm, such as a limited partnership, each person who controls the management or activities of the firm should be considered being a beneficial owner.

The above does not constitute an exhaustive list. FIATUM OÜ should review each customer against any other scenarios that are known to its management and employees.

FIATUM OÜ considers the following situations, which are indicative of a person actually is a beneficial owner.

1) All relationships that a person has with the customer's management bodies, including directors, should be taken into account, to identify whether the cumulative effect of those relationships places the individual in a position where they actually exercise beneficial ownership. For example:

> A director who owns important assets or has key relationships that are important to the running of the business (e.g. intellectual property rights), and uses this additional power to influence the outcome of decisions related to the running of the customer's business.

2) A person would be a beneficial owner if he or she is involved in the day-to-day management and direction of the customer's business activities. For example:

> A person who is not a member of the Management Board, regularly or consistently directs or influences a significant section of the board, or is regularly consulted on board decisions and whose views influence decisions made by the board.

3) A person whose recommendations are always or almost always followed by shareholders which hold the majority of the voting rights in the entity, when they are decided how to vote. For example:

> Where a founder of the entity no longer has a significant shareholding in it, but makes recommendations to the other shareholders on how to vote, and their recommendations are generally followed.

3. TRANSACTION SCREENING

3.1 GENERAL PROVISIONS

General

Each transaction of a customer is subject to transaction monitoring.

Enhanced transaction monitoring should apply to on a risk-based approach, and specifically to the following categories:

- politically exposed persons;
- high-risk customers;
- the customers who make suspicious activities, as specified in "Risk factors" subsection below;
- the customers operate above the transaction limits, which are specified below in "Transaction limits" subsection.

Transaction monitoring and enhanced transaction monitoring are conducted on a real time basis, i.e. where a transaction takes place or is about to take place.

FIATUM OÜ does not allow transactions to restricted countries that are listed in Appendix B "Restricted Countries" of this AML and TF Policy.

FIATUM OÜ does not allow cash transactions.

Transaction limits

The following transaction thresholds are imposed in relation to different categories of customer:

- transaction volume up to 1000 EUR per annum (or the equivalent in another currency (including cryptocurrency)), for the customers who has been subject to simplified due diligence;
- transaction volume up to 15000 EUR per annum (or the equivalent in another currency (including cryptocurrency)), for the customers who were subject to enhanced due diligence;
- transaction volume more than 15000 EUR per annum (or the equivalent in another currency (including cryptocurrency)) + source of funds for each transaction, for the customers who were subject to enhanced due diligence.

Risk factors

The following factors increasing risk of money laundering and terrorist financing are considered in the course of transaction monitoring:

- high value and frequency of transactions, especially when the customer holds multiple accounts;
- frequent cross-border transactions, especially when their scheme depend on counterparty;
- counterparties cannot be verified;
- the nature of the transaction is stated unclearly;
- transactions that are beyond face-to-face pattern;
- transactions with the use of multiple cards linked to the same account, particularly where the customer is able to pass on linked "partner" cards to anonymous third parties;
- segmentation of the business value chain, including the use of multiple agents and outsourcing, in particular to overseas locations;

- transactions do not correspond to the financial standing of the customer;
- transactions do not correspond to the customer's planned or regular business;
- the sources of funds in transactions are unclear;
- the customer, its client or main business partner make transactions to a country (territories) of low tax and duty;
- the customer has requested options for anonymity and international use;
- transaction of unusually large amount;
- the customer has requested for unlimited amount of transactions;
- large, complex transactions with a large number of parties;
- the monthly credit turnover is equivalent or exceeds the thresholds set in relation to the customer;

The listed above shall not constitute and exhaustive list.

Money laundering scenarios and "red flags"

FIATUM OÜ puts emphasis on stages of and related scenarios of money laundering and terrorist financing. In the course of transaction monitoring, FIATUM OÜ examines transaction patterns in order to detect risks of criminal activity. "Red flags" are indicative of such activity. At every stage of money laundering and terrorist financing, the following is under scrutiny.

Transactions without the use of debit cards	
Stage	**"Red flags"**
Placement - cash generated from crime is placed in the financial system. The funds are transferred or moved into other accounts or other financial institutions in order to separate the money from its criminal origin. When debit cards are used, a debit card may be obtained without exposing identity, and with the purpose to add illicit money into such debit card. Agents may be hired at this stage. Such agents are intended to deposit funds into multiple debit cards.	a) Transactions from multiple accounts for the same receiver; b) transactions from one account to multiple receivers; c) transactions coming from accounts created by auction houses, betting sites or e-wallets or e-wallet mainly used by gambling and betting sites; d) transactions from pre-paid credit cards; e) depositing funds into multiple debit cards, especially when that is done by a hired agent.
Layering – money passes through complex transactions, often between different entities, probably in multiple jurisdictions. The funds are transferred or moved into other accounts or other financial institutions. When debit cards are used, funds are transferred among a significant amount of debit cards.	a) Selling assets or switching to other forms of investment; b) transferring money to accounts at other financial institutions, c) wiring transfers abroad (often using shell companies), d) depositing cash in overseas banking systems; e) allocating funds among multiple debit cards.

Integration – the funds are made reappear in legitimate funds or assets through purchases, inheritance, loan payments, etc. Debit cards may be used to repayment of loans, or as a pledge to apply for loan.	a) Outgoing transactions to countries with not transparent banking systems, which were known as "offshore" countries; b) customers are using funds of a sales of assets like as house or jewelry; c) customers are using funds for purchases of real estate, buying stakes in companies or other large assets; d) incoming or outgoing transactions from private people to a company; e) transfers from prepaid credit cards to bank accounts; f) transactions made to repay loans, or to provide a pledge for loan repayment.

3.2 ENHANCED TRANSACTION MONITORING

FIATUM OÜ conducts enhanced ongoing monitoring in the following cases:

- there is reasonable suspicion that the customer is a shell bank or a credit or a financial institution which is known to allow its account to be used by a shell bank;
- the customer is a financial institution;
- the customer's beneficial owner is a politically exposed person (PEP), or whose beneficial owner is a family member of PEP or the person known to be close associate of PEP, or is suspected to be any of such persons;
- the customer is classified as a high-risk customer, or suspected to be of high risk;
- the customer's beneficial owner is suspected to be related in any of the restricted countries specified in Appendix B "Restricted Countries" of this AML and TF Policy;
- the customer or its beneficial owner is involved in a business sector with a high risk of corruption, or where cash transactions have an essential role, such as forex trading, adult – related activities, unlicensed pharmaceutical, metallurgy, etc.

The lower transaction thresholds may be imposed, as MLRO may decide.

3.3 CRYPTO TRANSACTION MONITORING

The Company is exposed to two primary aspects of transactions, the first is the inbound transactions, the receipt of Crypto from clients to fund the clients intended crypto spending. The second is the outbound payments, whether with cards or bank payments. There is a technical third issue raised by the partners acting to interchange the crypto for fiat, but this will be dealt with by only operating with a small number of regulated or otherwise reputable partners.

Inbound Crypto Transactions

Company monitors on an ongoing basis all transactions (however complex, unusual, suspicious, large or other transactions). The Company's outsourced partner for undertaking transaction analysis is Chainalysis and their capability covers Bitcoin, Ethereum, Litecoin and other major coins.

In essence, Chainalysis takes an entire history of coin transactions and runs clustering algorithms over them to estimate wallets. Two different clustering or heuristic techniques are used to estimate wallet addresses, Co-spend and Behavioural, this forms the basis for transaction monitoring activity to be undertaken by Compliance.

Note SAR's are not automatically submitted as a consequence of alerts issued by our transaction monitoring activities; rather, the requirement is to submit after monitoring, in essence detecting those transactions that fall outside the expected parameters for that profile of client(s), these being included in our exception alerts and after suitable investigation of the transactions, values, sources of transactions.

Transaction reporting capability will be calibrated to issue exception alerts on transactions that fall outside normal parameters or those that may flag higher risk provenance i.e. emanating from dark net markets.

The Company shall monitor the activities of any individual involved in the activity that results in a SAR for repeated behaviour and will report on recurring activity as appropriate to the FIU.

Comprehensive guidance on reporting SAR's may be found in the FIU website which outlines how SAR' may reported online or manually.

Outbound Transactions

The other side of the Company's transaction risk is where we transmit fiat cash to third parties, both card payments and bank payments.

We are working to extend our systems to allow us to build a client profile that allows us to monitor the behaviour of the client, as well as monitoring the client in general against adverse media lists (not just PEP lists).

All individual transfers out by bank transfer should be run against blacklists of bank accounts available from anti money laundering system providers.

Any attempts to send funds to known blacklist payments accounts will be blocked and will result in a referral to compliance for investigation and the possible raising of a SAR.

Customer behaviour profiles will signal unusual information that can be blocked unless the client is able to explain to the satisfaction of Compliance.

3.4 PROCEDURE

FIATUM OÜ operates transaction screening through special software and appoints responsible employees to run such software and perform non-automatically, when necessary.

The software is represented by Sum&Substance, which operates 24/7.

Should any of the risk factors appear within the software, the responsible employee becomes aware of it and immediately reports a case of suspicious activity to MLRO. The suspicious transaction is blocked. The MLRO investigates the case and takes any (including several) of the following decisions:

- to allow the transaction;
- to leave the transaction blocked;
- to freeze the account;
- to request the source of funds;
- to impose enhanced ongoing monitoring upon the customer's transaction;
- to ban the account;
- to report the case to competent authorities.

4. DESCRIPTION OF CRYPTO ACTIVITIES

Operations Overview

- Each Company account is linked to a unique blockchain address – "Transaction Wallet";
- All the crypto funds deposited to the user's transaction wallet are transferred to a "hot" wallet that securely accumulates all users' crypto currency holdings;
- When a crypto/fiat transaction occurs, market risk is eliminated by hedging with liquidity providers.

Multi-currency Transaction Wallets

Crypto to fiat payments overview

Providing wallets to customers ensures that acceptable cryptocurrencies are immediately available for exchange into fiat. Each wallet provided to the clients enables them to pay with cryptocurrencies using existing payment mechanism and wallets are managed and accessible solely through Company interfaces.

Each wallet will consist of an account established for a Client on the Company's records to reflect the amount of each type of cryptocurrency that the Company holds in a custodial fashion and which is then available to purchase fiat. For each type of permitted cryptocurrency, the Company will maintain three separate multi-signature cryptocurrency wallets. The Company will use these Wallets only for the purpose of holding all cryptocurrency the Company receives in connection with the Wallets in a pooled custodial manner on behalf of its Clients, with the Company maintaining a sub-account ledge noting the amount of each type of cryptocurrency that it holds for each Client in the pooled Wallets.

In addition, the Company will generate Client specific public keys for the relevant pooled custodial wallet used by the Company to receive cryptocurrency. Clients will send cryptocurrency to these addresses, which will allow the Company to track such transfers on an individual Client basis.

The transfer of cryptocurrency assets depends upon a confidential transaction signing "key" which is associated with the wallet that holds the assets. Without this key the accounts are inaccessible, however possession of the key for cryptocurrencies provides the key holder with ability to immediately & irrevocably transfer the associated cryptocurrency.

The use of multi-signature wallets, which allow cryptocurrency assets to be assigned to a wallet that is linked to multiple private keys, with a majority of the keys needed to produce a valid transaction.

The Company uses 2-out-of 3 multi-signature approach, in which two keys are held online by the Company and one held offline for back-up purposes. When producing a new transaction, the transaction will be signed with the two online keys and then broadcast to the appropriate blockchain network for validation. A key advantage of a multi-signature wallet is that the wallet can remain on-line while providing a heightened level of security since more than one key is needed to authenticate any given transaction

Transfer of Cryptocurrency to a client's wallet

To transfer cryptocurrency to a client wallet, a Client will make a request, through their preferred interface. The Company will then generate a unique transfer address, associated with one of the pooled custodial wallets used by the Company to receive Crypto currency and to which the client will send their cryptocurrency.

The client will then create a transaction transferring cryptocurrency from the client's external wallet to the unique transfer address and submit it to blockchain to be validated. Once validated by blockchain, thus finalizing the transfer of the cryptocurrency to the unique transfer address and this the associated pooled custodial wallet used by the Company to receive cryptocurrency, the Company will then credit the Client's Wallet – that is the Company's sub-

account ledger noting the amount of cryptocurrency held for the Client with the relevant type and amount of cryptocurrency.

The Client is now in a position to use their cryptocurrency to convert into fiat and spend as the wish, Company, upon completing the conversion, will send fiat to either:

- to the customer's account;
- directly to the merchant;
- to a partner bank to replenish the credit balance;
- transferred to the client's bank card;
- to a third party to complete payments; or
- card payment solution.

Contactless payments through mobiles phone vendors will be offered in addition to payment cards.

Transfer of Cryptocurrency from a client's wallet

To transfer cryptocurrency from their wallet held with the Company to their external wallet, a client would log-on to their preferred interface, enter their request, authenticate and the submit to the Company.

Upon receipt of the transfer request the Company would check the requested transfer amount against the available balance in the Client's Wallet and perform any checks required under the AML Procedure.

Once completed the Client's Wallet balance will be reduced accordingly and the Company initiates a transfer of the relevant cryptocurrency by submitting an authenticated transaction i.e. one signed by 2 of the 3 keys as noted previously, to be validated by blockchain. Once validated, the transfer of the cryptocurrency to the Client's external wallet will be complete.

5. POLITICALLY EXPOSED PERSONS (PEPs)

PEPs are regarded as high-risk customers.

Within the period when a PEP holds its status and the period of 12 months when the PEP ceases to hold its status, he or she is subject to:

- enhanced due diligence;
- enhanced transaction monitoring;
- obligation to prove the source of funds for transactions.

FIATUM OÜ ensures that all accounts of PEP are approved by MLRO in overall or each separately.

FIATUM OÜ runs a check against several databases to verify if the customer is a PEP. In addition, PEP status of the customer is monitored with the use of Sum&Substance, which is described in Appendix C "Sum&Substance" to this AML and TF Policy.

FIATUM OÜ requests from each customer a written declaration of its PEP status.

For identification of a PEP, the following sources are used by FIATUM OÜ:

- the data of central public registers (including those held in European e-Justice Portal, the European Business Register, registers held by competent authorities of certain European countries) concerning shareholders of the legal entity (in the European Union);
- information from the contracting parties, where available;
- the World Bank List of Fragile States, Transparency International's Corruption and Perceptions Index (CPI), the FATF list of jurisdictions, FATF and FSRB mutual evaluation reports as well as the International Monetary Fund (IMF) and the World Bank AML/CFT assessments to assist with analysis of risk factors, such as country risk;
- EveryPolitician.org, Rulers.org, LittleSis.org;
- commercial PEP database providers, namely NameScan and its data Sapphire Checks, that utilises Acuris Risk Intelligence's Database of PEP and Sanctions;
- media and journals;
- Internet and search engines.

The provisions of this section should apply to family members of PEP and the persons known to be close associates of PEP, as well as to the persons who has, at any time in the preceding year, been known to be a PEP, and the persons who are suspected to be a PEP.

6. SANCTIONS SCREENING

FIATUM OÜ screens each customer against:

- the UK HM Treasury sanctions list;
- the US Office of Foreign Assets Control sanctions list;
- the EU sanctions list (administered by the High Representative of the European Union for Foreign Affairs and Security Policy and the European Commission);
- the UN sanctions list (administered by the United Nations Security Council).

The Firm uses Sum&Substance AML screening solution for quick identification of persons associated with criminal activity or those who are prohibited from certain industries and activities. Sum&Substance allows to screen each customer against thousands of fitness and probity, global and national sanctions lists: OFAC, HMT, UN, and many more and carry out real-time monitoring as well.

The scope of sanctions screening includes, without limitation, the following:

- appearance of the customer on the sanctions lists;
- engagement in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by the United States of America, the European Union, the United Kingdom and the United Nations.

Should onboarding process in relation to any customer be initiated, FIATUM OÜ screens the customer on a daily basis, until the customer relationship ends.

Each transaction is subject to sanctions screening, regardless of value of the transaction and the customer's risk status or other characteristics. No transaction is effected unless sanctions screening is conducted via special software.

Sanctions screening is run by an employee appointed by FIATUM OÜ. The employee is responsible for running the software and reviewing screening output. If a customer is found in any of the above listed sanctions lists, he or she informs the MLRO immediately. The MLRO investigates whether there is risk of money laundering or terrorist financing in the case or not, and decides to reject the transaction and (or) block the customer's assets, or to allow it.

Customer's account would get blocked by MLRO and senior management would be notified.

The MLRO is obliged to investigate each case of rejected transaction and determine possible money laundering or terrorist financing risks. Upon such investigation, the MLRO reports to the Director regarding the customer who is suspected in money laundering or terrorist financing activities and recommends the Director what further actions should be taken.

Upon the MLRO's recommendation, the Director decides to refuse to continue the customer relationship or to continue them.

The MLRO reports each case of suspicious activity to competent authorities, regardless of the Director's decision on the suspected customer.

Sum&Substance is used for sanctions screening. The software keeps track of all recent amendments that come into force (as the US Office of Foreign Assets Control, the High Representative of the European Union for Foreign Affairs and Security Policy, the European Commission, the United Nations Security Council, and other competent authority decides).

Description of Sum&Substance is provided below in Appendix C "Sum&Substance" to this AML and TF Policy.

7. PROHIBITIONS ON CUSTOMER RELATIONSHIPS

General

FIATUM OÜ does not enter into, or does not continue, any customer relationship with the customers, who(-se):

- identity cannot be verified, or who refuses to provide information required to verify identity required for account opening purposes, or who has provided information that contains inconsistencies that cannot be resolved after further investigations;
- has falsified documentation or provided false, incomplete or incorrect information;
- uses anonymous accounts or accounts with pseudonyms or numbers rather than those bearing real names;
- beneficial ownership cannot be determined, including where the customer's entity structure is convoluted enough to prevent true and correct identification of such ownership;
- is a credit institution of a financial institution which is known to be a shell bank, or allow its accounts to be used by a shell bank;
- is involved in any of the prohibited activities, that are specified in this AML and TF Policy;
- is related to any of the restricted countries, as they are listed in the Appendix B "Restricted Countries" of this AML and TF Policy;
- is on relevant sanctions list specified in Article 5 "Sanctions Screening" of this AML and TF Policy.

This above list is not exhaustive. FIATUM OÜ may refuse to enter into or continue customer relationship with any customers who is reasonably suspected in money laundering or terrorist financing.

Prohibition to cooperate with shell banks

"Shell bank" means a credit institution or a financial institution, or an institution engaged in equivalent activities to those carried out by credit institutions or financial institutions, incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-making and management, and which is not a part of a financial conglomerate.

FIATUM OÜ does not enter into, or continues a corresponding relationship with either a shell bank or a credit or a financial institution which is known to allow its account to be used by a shell bank.

Banned customers

FIATUM OÜ does not provide its services to the companies, if their activity relates to the following:

- counterfeit goods / replicas;
- drug trafficking including chemicals used to manufacture synthetic drug or drugs;
- production or activities involving harmful or exploitative force on child labor;
- production, trade, storage, or transport of hazardous chemicals;
- any business relating to pornography or prostitution;
- abusing confidential or material, non-public information;
- trading of animal fur, bones and ivory;
- cultural objects like sculptures, statues, antiques, collectors' items, archeological pieces;
- production or trade in weapons and munitions;
- trading of Fireworks, explosives and Nuclear Weapons;
- human trafficking;
- human body parts and pathogens;
- bailiff services;

- jewel, gem, precious metal dealers without license;
- non-licensed counselling centers;
- timeshare, timeshare maintenance;
- pyramid selling;
- illegal telecommunication devices;
- non-licensed lawyer services and/or advice;
- non-licensed gambling;
- most-significant bit (MSB) activities;
- crowdfunding;
- fortune tellers, tarot card and horoscope readers, psychics;
- dating: subscription-based dating websites which do not have genuine, underlying matches or products;
- real estate / property clients: dealing in property that are not regulated by any AML regulations;
- trust and company service providers: their dealing is not regulated by any AML regulations.

8. AML RISK MITIGATION MEASURES

ID	MITIGATION MEASURE
AML/R1	SDD accounts have a lifetime relationship limit and are subject to enhanced ongoing monitoring. SDD accounts are clearly marked within the system and SDD limits are enforced on such accounts.
AML/R2	As part of the verification process, we check customer's addresses against various databases from industry's leading information provider – Sum&Substance. When a client reaches a certain account threshold, a check is automatically run and is reviewed by a compliance specialist. A certified third-party provider is used to access databases to run background checks. Account thresholds are the following: ● SDD account threshold: annual transaction volume up to 1000 EUR; ● EDD account threshold: annual transaction volume up to 15,000 EUR; ● EDD + source of funds threshold: annual transaction volume more than 15,000 EUR.
AML/R3	We run image manipulation tests on all documents that are received from the customer. As soon as we receive documents from the customer, we run a check if documents were altered or amended using the following algorithms: ● Signature Analysis; ● Thumbnail Analysis; ● Error Level Analysis; ● JPEG Ghosts; ● Block Artefact Grid; ● Stamp.
AML/R4	The user would not be able to access the majority of services and would have SDD limits enforced on their accounts. Such accounts are reviewed by trained compliance specialists; extra background checks will be completed.
AML/R5	Real-time monitoring, where transactions and/or activities can be reviewed as they take place or are about to take place. After the event, through some independent review of the transactions and/or activities that a customer has undertaken. It flags up transactions and/or activities for further examination with an appropriate Risk ID. These reports are reviewed within 24 hours by the designated compliance officer and appropriate action is taken on the findings of any further examination (account suspension, senior management notification, risk-profile change).
AML/R6	Real-time monitoring, where transactions and/or activities can be reviewed as they take place or are about to take place. It flags up transactions and/or activities for further examination based on the account historical transaction volume. All users are obliged to verify the device used for account access using device fingerprinting technology upon reactivation of dormant accounts. Extra checks are being carried out, including enhanced transaction monitoring and lower velocity limits.
AML/R7	We do not onboard clients from restricted jurisdictions: Appendix B "Restricted Countries". In order to get the full use of the account, customers must successfully pass the account verification procedures. Proof of Address documents from high- risk countries are not accepted. We limit access from high-risk jurisdictions based on the IP/location data.

AML/R8	We run a check against several databases to verify if the client is a PEP. Enhanced due diligence is applied to such customers. Senior management approval is necessary in order to interact with such person. PEP customers are also subject to enhanced ongoing monitoring of the business relation. Source of wealth and source of funds which are involved in the business relationship or occasional transaction are verified with reference to documents.
AML/R9	Prior to onboarding a client, we check customers against sanction lists. If a customer appears on the sanction list, it would not be possible to set up an account with us or to use any services. Customer's account would get blocked by MLRO and senior management would be notified.
AML/R10	Ongoing screening of existing customers against sanction lists. If a customer appears on the sanction list, all funds will be frozen and a report will be sent out to the FIU for further course of actions.
AML/R11	Possible sanction list matches are filtered for a review. Our system will highlight any possible matches and all cases will be reviewed by trained compliance officers. Additional documentation will be requested before the customer gets on board to make sure that it is a false-positive match.
AML/R12	Card activation is a separate step that has to be done by the customer. All of our customers would need to activate the card prior to use. During the activation, personal information will be asked and checked against our internal records.
AML/R13	Automated address monitoring. If the card order has the same delivery address as the other user already has, an application will be put on hold and sent for a review by a compliance officer.
AML/R14	Card limits are signed off by BIN sponsors and enforced by Processor rules. In order to have increased card limits, the customer would have to fully verify the account. Unverified customers do not have access to higher limits.
AML/R15	Account/velocity parameters are signed off by BIN sponsors and enforced by Processor rules. An access to higher limits is given only to the fully verified accounts, based on the decision of a compliance officer and subject to all the necessary checks being carried out. There is no option for an automatic increase of the limits.
AML/R16	Third-party account top ups are prohibited and get refunded back to the payer. Third-party deposits into the account are prohibited and would get refunded back to the sender.
AML/R17	Corporate accounts have to pass EDD in order to be able to top up the PM prefunding account. Card loads are limited to corporate loads only, with all the corporate accounts being fully EDD.
AML/R18	Unusually high load would flag the account. Whenever a customer is making an unusually high load, such an account does get flagged and then reviewed by the trained compliance specialist. A source of funds confirmation would be obtained.
AML/R19	We use the automated transaction monitoring system which uses a variety of techniques to detect any unusual/suspicious activity. Based on third party CurrencyCloud we will screen each transaction and approve/reject it in real time.
AML/R20	Relevant employees undergo training and must report any suspicious activity to the compliance officer. If necessary further reports are sent to FIU. Reports are generated automatically and are reviewed by the MLRO to make sure the submission is done on time.
AML/R21	All members of staff are aware that disclosing information regarding internal or external report has been made a criminal offence.
AML/R22	Our system analyses client information during the login process, device fingerprint, IP address and location are checked against our records. Customers are notified about the importance of use

	of 2FA authentication in order to prevent unauthorised access to the account
AML/R23	We use the automated transaction monitoring system which uses a variety of techniques to detect any unusual/suspicious activity and to block such cards in case of the theft. There is an option to block the card via the web interface or on a mobile app.24/7 IVR line is available in case a customer doesn't have access to the internet.
AML/R24	Card activation is a separate step that has to be done by the customer. All customers would need to activate the card prior to use. During the activation, personal information will be asked and checked against internal records.
AML/R25	Company holds a substantial reserve in order to allocate trained compliance officers in a timely manner. We keep an adequate staff pipeline in order to manage the product should the amount of resources required increase drastically.
AML/R26	All the compliance officers must be certified by an internationally recognised AML training institution. (e.g. ICA) All compliance officers undergo rigorous background checks and must obtain an internationally recognised certificate in order to manage the AML procedure.
AML/R27	All the cardholder activity is logged and securely stored in an encrypted form in order to meet PM's recordkeeping requirements.

9. MLRO'S ROLES AND RESPONSIBILITIES

All staff must take steps to ensure compliance with this policy and ensure that they fully understand the material contained in this document.

Responsible for overall compliance policy of FIATUM OÜ and ensuring adequate resources are provided for the proper training of staff and the implementation of risk systems. This includes computer software to assist in oversight.

The MLRO (Money Laundering Reporting Officer) holds copies of all training materials. Updated AML training is given annually. Records of all training including dates delivered and by whom are kept both centrally and on staff personnel files.

Senior management will be sent monthly updates by the MLRO on compliance. They will also receive and consider the annual MLRO report and implement any recommendations made within it. Assistance may be given to the MLRO in the preparation of the AML manual.

The MLRO of FIATUM OÜ is also holding the formal position of CRO (Chief Risk Officer) organizing the company risk management using the risk mitigation and fraud prevention tools and procedures. FIATUM OÜ has a risk-based approach that is why we have chosen our MLRO to become the company CRO to guide and lead us in this way.

All issues related to any noticed suspicious activity must be referred to MLRO in the first instance. The duties of the Money Laundering Reporting Officer include:

1. Monitoring the firm's compliance with AML obligations;
3. Being designated for, and accessible to, receiving and reviewing reports of suspicious activity from employees;
4. Considering of such reports and determining whether any suspicious activity as reported gives rise to a knowledge or suspicion that a customer is or could be engaged in money laundering or terrorist financing;
5. Overseeing communication and training for relevant employees;
6. Ensures that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports are filed. The Money Laundering Reporting Officer is vested with full responsibility and authority to enforce the firm's AML program;
7. To receive disclosures from employees (also known as Suspicious Activity Report-SAR's);
8. To decide if disclosures should be passed on to the Financial Intelligence Unit (FIU);
9. To review all new laws and decide how they impact on the operational process of the company;
10. To prepare a written procedures manual and make it available to all staff and other stakeholders; 10. To make sure appropriate due diligence is carried out on customers and business partners;
11. To receive internal Suspicious Activity Reports (SARs) from relevant staff;
12. To keep and review records of all decisions relating to SARs appropriately;
13. To ensure that relevant staff receive appropriate training, when they join and that the receive regular refresher training on annual basis or if necessary;
14. To monitor business relationships and record reviews and decisions taken;
15. To make a decision on continuing or terminating trading activity with particular customer;
16. To make sure that all business records are kept for at least five years from the date of the last customer transaction.

Provision of Exemptions:

MLRO may only grant an exemption where he is clearly required, or where practical experience reveals that it is necessary to do so. All exemptions will be considered on a case-by-case basis.

FIATUM OÜ has adopted a risk-based approach to achieving its regulatory objectives and exemptions should not be considered as a way to avoid meeting our regulatory obligations.

Careful consideration will be given to issues of transparency, equity and competitive neutrality in issuing exemptions.

MLRO will assess the potential implications of applying for an exemption and aims to adopt a consistent approach, taking account of the facts and circumstances particular to each case. Request for Exemptions from standard Customer Identification Process requirements may be received from AML and Risk department in circumstances where, taking account of the CDD which has been obtained, MLRO is satisfied that the ML/TF risk has been adequately addressed.

AML and Risk department must use the "E-mail Exemption Request" when requesting an exemption from the Customer Identification Process. The completed e-mail must be sent to MLRO and must be approved by return of email by MLRO before any exemption can be provided.

10. COOPERATION WITH FINANCIAL INTELLIGENCE UNITS

General

MLRO shall be responsible for reporting to Financial Intelligence Unit. Each employee who is involved in activities under this AML and TF Policy, should immediately report MLRO of the cases where criminal acidity is seen.

Procedure

FIATUM OÜ reports to FIUs in a state of its business activities in the manner prescribed by the EU laws.

FIATUM OÜ promptly reports to FIUs when it knows, suspects or has reasonable ground to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing. FIATUM OÜ is obliged to promptly respond to requests by the FIU for additional information on such cases.

All suspicious transactions, including attempted transactions, must be reported immediately, including the events where it was discovered that the transaction is related to proceeds of criminal activity after the moment when such transaction was made. The scope of report should include the fact of suspected criminal activity, parties and beneficiaries of the transaction.

FIATUM OÜ ensures that it does not carry out any transactions which are known to be related to proceeds of criminal activity, and comply with instructions issued by FIU on such transactions.

11. AML SYSTEM AUDIT

11.1GENERAL PROVISIONS

AML system audit comprises technical compliance evaluation and implementation effectiveness assessment, that are guided by risk-based approach. AML system audit is arranged and supervised by MRLO at least once a year.

AML system audit may be carried out more often than once a year, if MRLO discovers insufficiency of AML and TF practices.

The stages of AML system audit are as follows.

11.2ANALYSIS OF EXTERNAL ENVIRONMENT

The objective of this stage is establishing the context, internal and external environment of AML system audit.

This stage involves review of regulatory environment, analysis of recent amendments to law and how they must be implemented, of AML status of FIATUM OÜ, and of the industry, including standard and best industry practices. More elements are included into consideration and the reference standard may be totally shifted. An analysis model like PEST can be adopted in this process.

Political factors may be additionally analyzed throughout this stage, including how the government intervenes in AML and the card industry.

Economic factors that are subject to review may include indexes and industrial data like interest rate, inflation rate, the ingredient of income, are emphasized for evaluating risks related to corruption, tax evasion and international trading, as well as some index or data like saving rate, the number of cards issued, the total and average transaction amount of cards, are directly linked to the usage of cards.

Social factors like employment rate and crime rate can be referred to anticipate predicate crime of money laundering, consumption custom like payment method can be referred to understand card overall cardholder behavior pattern.

Technological factors should be considered, including a currency tracking system, fraud prevention technology like a chip card, tokenization, and bio identification, will affect the money laundering and card features, as well as its derived products.

11.3ANALYSIS OF INTERNAL ENVIRONMENT

The following factors should be reviewed through this stage:

- management structure, and how it affects AML and TF practices of FIATUM OÜ;
- risk appetite;
- disadvantages of this AML and TF Policy;
- inefficiency of AML and TF procedures, especially effectiveness of transaction limits, KYC procedures, transaction screening, due diligence procedures, PEP-related procedures.

11.4 EVALUATION OF TECHNICAL COMPLIANCE

The process of evaluation of technical compliance involves cross check if an AML framework includes policy and procedure as it should have and all components have been covered (e.g. organization structure, customer identification and acceptance, transaction monitoring and reporting, training, recordkeeping, and auditing).

11.5 ASSESSMENT OF IMPLEMENTATION EFFECTIVENESS

Implementation procedures are examined with regard to the requirements set by this AML and TF Policy. Records of procedures made by the employees involved in AML and TF practices, the system of "red flags", and SAR reports are reviewed.

11.6 DEFINING RESIDUAL RISK AND PROPOSAL OF IMPROVEMENT

Testing or auditing procedures are applied in order to calculate residual risk, expose shortage and provide opinions on improvement.

Once residual risk has been worked out, the outcome is compared with pre-defined expectations, so that the shortage can be exposed, and then a recommendation for correction or improvement is laid by MRLO before the Management Board for approval.

12. TRAINING OF EMPLOYEES

FIATUM OÜ ensures that its employees involved at anti-money laundering and counter terrorist financing meet relevant Training and Competence requirements and are competent enough for carrying out relevant activities.

MRLO is responsible to oversee that the above requirements are fulfilled, on an annual basis.

MRLO develops and maintains training schedules for the employees and arranges refresher training annually.

MRLO supervises daily performance of the employees and raises disciplinary issues, when necessary.

The following requirements should be met:

- the employees are familiar with the laws on money laundering and terrorist financing adopted on domestic and international levels;
- the employees attend lectures, case studies and are successful in taking tests;
- the employees are capable of recognizing and dealing with suspicious activities;
- the employees properly fit high risk roles led by a risk-based assessment;
- the employees know the peculiarities of cryptocurrency exchange;
- the employees are able to identify and minimize risks arising when working with cryptocurrency.

FIATUM OÜ ensures that its employees are aware of the typologies that criminals use, as they are identified by relevant authorities, as well as the scenarios defined to detect them, the red flags to identify them and the investigation techniques to validate them.

APPENDIX A RECORD KEEPING

As per the Compliance, all necessary information regarding the transactions has to be maintained properly, to permit reconstruction of individual transaction, including the following information:

a) the nature of the transaction;
b) the amount of transaction and the currency in which it was denominated;
c) the date on which the transaction was conducted; and
d) the parties to the transaction.

Data to be collected properly and efficiently must be retrieved easily and quickly whenever required or when requested by the competent authorities.

Records must be maintained for at least 5 (five) years from the date of transaction between the FI and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for connection of persons involved in criminal activity.

Records, related to the client identification procedures, ultimate beneficial owner and his address (e.g. copies of documents like passports, identity cards, driving licenses, utility bills etc.) obtained while opening the account and during the business relations, as well as business correspondence are properly archived for at least 5 (five) years after the business relations are closed.

The identification records and transaction data should be available to the competent authorities upon request. Background including all documents/office records/memorandums pertaining to all complex, unusual large amounts transactions and all unusual patterns of transactions, which have no substantiated economic reason or visible lawful purpose which should be thoroughly examined and scrutinized at branch as well as Principal Officer level must be properly recorded.

Such records and related documents should be available to assist auditors in their day-to-day work relating to scrutiny of the transactions and also to relevant authorities. These records are required to be preserved for 10 (ten) years as required under Compliance.

List of records to be kept:

1. Suspicious transaction report records (five years);
2. Records of transactions of below €10,000 regular check, above €10,000 enhanced check (five years);
3. Foreign currency exchange transaction records (five years);
4. Account opening records (five years from account closure date):
    a. Signature cards;
    b. Intended use of an account;
    c. Accounts for individuals or entities other than corporations;
    d. Accounts for corporations;
    e. Account records created in the normal course of business;
5. Account records (five years from account closure date):
    a. Account statements;
6. Card account opening records (five years from account closure date);
7. Reasonable measures records (described below).

When reasonable measures are unsuccessful, the following information must be recorded:

a) the measures taken;
b) the date on which each measure was taken;
c) the reasons why the measures were unsuccessful.

APPENDIX B RESTRICTED COUNTRIES

In order to meet anti-money laundering and sanction screening requirements, currently FIATUM OÜ cannot make payments to the following countries:

Afghanistan Republic	Mongolia Republic
Algeria People's Democratic Republic	Mozambique Republic
Angola Republic	Myanmar Union Republic (formerly Burma)
Bahamas Commonwealth	Namibia Republic
Belarus Republic	Nigeria Federal Republic
Bolivia Plurinational State	North Korea Democratic People's Republic
Botswana Republic	Northern Cyprus Turkish Republic (Lefkosa)
Burkina Faso Republic	Pakistan Islamic Republic
Cambodia Kingdom	Palestinian Territory (State of Palestine)
Central African Republic	Panama Republic
Columbia Republic	Serbia Republic
Congo Democratic Republic	Sierra leone Republic
Cote d'Ivoire Ivory Coast	Somali Federal Republic
Crimea Region Republic	South Sudan Republic
Cuba Republic	Sri Lanka Democratic Socialist Republic
Eritrea State	Sudan Republic
Ethiopia Federal Democratic Republic	Swaziland (Eswatini Kingdom)
Ghana Republic	Syria Arab Republic
Iceland Republic	Timor-Leste Democratic Republic (East Timor)
Iraq Republic	Trinidad and Tobago Republic
Iran Islamic Republic	Tunisia Republic
Lebanon Republic	Turkmenistan Republic
Liberia Republic	Vanuatu Republic
Libya State	Yemen Republic
Mali Republic	Zimbabwe Republic
Mauritius Republic	

***Please note the above countries are subject to change.**

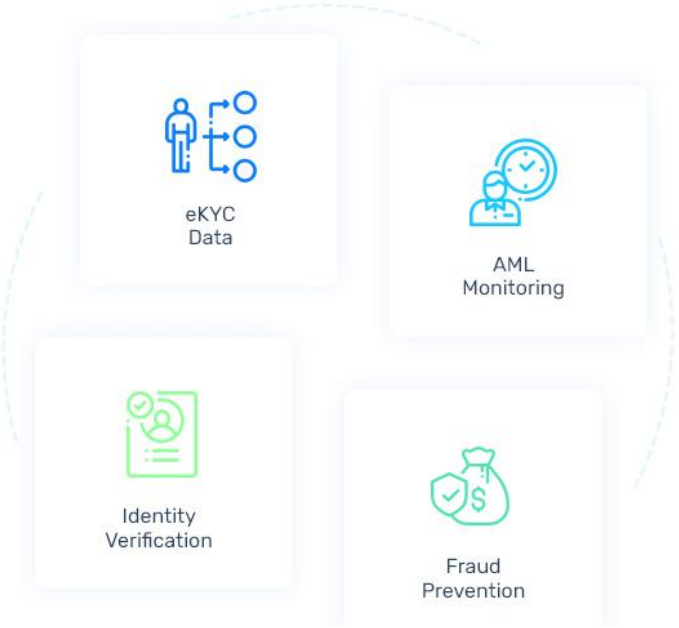
APPENDIX C SUM&SUBSTANCE

Sum&Substance system is used to identify, investigate and rapidly react to suspicious behaviours in real-time or retrospectively.

Spotting outlier activity and uncovering risk at an entity or transaction level

Better identify changes in behaviour over time and alerts to typical money laundering scenarios, with deeper insight into the risk patterns of all parties in the transaction.

Compliance with the requirements of regulator, banking partners and auditors with an electronic audit trail of all system and user actions with date and time stamps. Spotting patterns and outliers by monitoring current transactions alongside historic transaction and behavior data.



Improvement of operational efficiency and reduction of false positives by 70%

Risk-based approach and configure rules and scenarios to customer and transaction risk levels, resulting the notification on the transactions that matter. By viewing alerts at an entity or transaction level, results to transactions assessment in the context of the customer, whilst significantly reducing the number of alerts to review.

Configurable cloud solution, tailored to the business model

Avoid Business Fraud

Conduct ongoing screening to identify high risk businesses in realtime.

By utilizing analytics to automatically trigger relevant alerts and drive internal workflow, high-risk transactions are stopped as they happen in real-time, or retrospectively via batch upload.

Benefit from flexible API integration and adapt to risks at reduced cost, without relying on technology teams.

By utilizing Sum&Substance, we use real-time data with updates as often as every 15 minutes. Better segmentation and screening data according to the risk policy, reducing false positives in the process as well as giving compliance team much richer insights.

Customers are onboarded and funds cleared in minutes, with customer satisfaction and feedback much improved.

The platform has the option to effectively consolidate transactions into a single meaningful analysis, to assess transactions in the context of the customer.

By viewing alerts at an entity or transaction level, it is able gain deeper insight into the risk patterns of all parties in the transaction, while significantly reducing the number of alerts the team has to review.

Users can better identify changes in behavior over time per entity and spot suspicious behavior faster.

Features

- One simple API integration
- Unique, innovative toolkit of due diligence tools to manage your compliance and risk
- Flexible commercial agreements for businesses of all sizes
- Efficient project delivery
- Fewer supplier contract agreements
- Large choice of data providers to meet requirements
- Single contract & billing point
- Increased service access at ‘the flick of a switch’