VERSION 01.1(2022)

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING COMPLIANCE POLICY

P-01.00

Transactive Systems UAB

2021

Approval table

Approved by	The Board
Approved on	November 4th, 2021
Document owner	Head of Compliance
Next review	Q4 2022

Contents

1 Introduction

This manual is for the use of the management and employees of Transactive Systems UAB as a guide to their Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) responsibilities.

In particular, it contains information which all members of staff need to be aware of in order to prevent the business being used to launder the proceeds of crime or for terrorist financing and any activity that facilitates Money laundering or the funding of terrorist or criminal activities and to comply with all applicable requirements under the Lithuanian AML/CTF framework:

Key elements of the Lithuanian AML/CTF framework are:

- Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania No VIII-275 of 19 June 1997 (as amended) (the Law);
- Resolution of the Bank of Lithuania No 03-17 of 12 February 2015 on the approval of the Instructions for the Financial Market Participants Aiming to Prevent Money Laundering and/or Terrorist Financing (as amended) (the Instructions);
- Order No V-314 of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania (FCIS) of 30 November 2016 on the approval of Technical Requirements for the Customer Identification Process Where the Identification is Performed Remotely by Electronic Means Facilitating Video Streaming approved by (as amended) (the Technical Requirements);
- Order No V-129 of the Director of the FCIS of 4 September 2017 on the approval of the Rules on Management of Registration Logs of Monetary Operations, Transactions and Customers;
- Order No V-240 of the Director of the FCIS of 5 December 2014 on the approval of the List of Criteria for the Recognition of the Money Laundering and Suspicious Monetary Operations or Transactions;
- Order No V-273 of the Director of the FCIS of 20 October 2016 on the approval of the Supervision Instructions on the Appropriate Implementation of International Financial Sanctions under the Regulatory Scope of the FCIS;
- Order No V-129 of the Director of the FCIS of 21 May 2015 on the approval of the Forms and Schemes of the Provision of Information, provided under the Requirements of the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, and Recommendations on Filing of the Forms;

Institutions responsible for the prevention of Money laundering and Terrorist financing are the FCIS and the Bank of Lithuania.

In this document references to “we”, “firm”, “Transactive” and “Transactive Systems UAB” refer to Transactive Systems UAB.

Transactive Systems UAB is a risk averse company which implements and maintains controls in order to minimise ML/TF risk to maximum extent possible in activities of the firm. Where we cannot ensure the sufficient implementation of such controls, Transactive Systems UAB will decline to enter a Business relationship with the potential Customer.

2 Regulatory Context

2.1 Money Laundering and Terrorist Financing

Money laundering has various definitions but it is always understood as the illegal process seeking to conceal the origins of money obtained illegally by passing it through a complex sequence of payment transfers or commercial transactions knowing that such money (property) is derived from criminal activity of from the act of participation in such activity.

Money laundering often occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, in firms situation it would be relevant when, for instance, funds are deposited into accounts of the Customer at the firm. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin (e.g. when the Customer of the firm transfers funds from its e-money account to payment accounts of other recipients within or outside Transactive payments environment). At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses (e.g. when the Customer purchased something using the funds placed within its e-money account).

Terrorist financing means the provision or collection of funds, by any means, with the intention that they should be used (or in the knowledge that they are to be used) in full or in part in order to carry out any of the offences may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are one of possible and mostly seen differences between terrorist financiers and traditional criminal organisations engaging in Money laundering. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

2.2 The Regulatory Background

This policy implements the Law and other legal acts specified in Section 1 above.

Other laws and regulations of Lithuania include:

- Law on the Implementation of Economic and other International Sanctions of the Republic of Lithuania No IX-2160 of 29 April 2004 (as amended);
- Criminal Procedure Code No IX-785 of the Republic of Lithuania of 14 March 2002 (as amended);
- Resolution of the Government of the Republic of Lithuania No 178 of 15 March 2017 on the approval of the description of requests to carry out prior authorization to perform international money transfers with persons, entities and organizations of the Democratic People's Republic of Korea;

- Criteria of recognition of terrorist financing published by the State Security Department of the Republic of Lithuania;
- Other applicable legislation.

2.3 Definitions

In this document,

"**Close associate**" shall mean: 1) a natural person who, together with a person who performs or performed Prominent Public Functions, participates in the same legal entity or maintains other business relations; or 2) a natural person who is the only Beneficial owner of a legal entity or an unincorporated organisation established or operating de facto with a view to receive economic gain or other personal benefits for a person who performs or performed Prominent Public Functions.

"**Immediate family members**" shall mean a spouse, a person with whom partnership has been registered, parents, siblings, grandparents, grandchildren, children and children's spouses, persons with whom children have registered partnership.

"**Person**" shall mean a natural or legal person of the Republic of Lithuania or a foreign state, an undertaking of a foreign state.

"**Business relationship**" shall mean a business, professional or commercial relationship of a Customer and Transactive regarding the provision of e-money and payment services which is expected, at the time when entering into Business relationship, to have an element of duration.

"**Correspondent relationship**" shall mean:

(a) the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;
(b) the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

"**Financial institutions**" shall mean credit institutions and financial undertakings as defined by the Law on Financial Institutions of the Republic of Lithuania, payment institutions as defined by the Law on Payment Institutions of the Republic of Lithuania, electronic money institutions as defined by the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania, currency exchange operators as defined by the Law on Currency Exchange Operators of the Republic of Lithuania, crowdfunding platforms operators as defined by the Law on Crowdfunding of the Republic of Lithuania, peer-to-peer platforms operators as defined by the Law on Consumer Credit of the Republic of Lithuania and the Law on Credit related to Real Estate, insurance companies, engaged in life-insurance activities, as well as insurance brokerage, engaged in life-insurance brokerage activities as defined by the Law on Insurance of the Republic of Lithuania, as well as investment companies with variable capital and collective investment undertakings, designed for well-informed investors and management companies managing only the aforementioned collective investment undertakings of the Law on Collective Investment Undertakings

Designed for Well-Informed Investors; branches of these foreign financial institutions, established in the Republic of Lithuania, as well as payment institutions and electronic money institutions, the headquarters of which are in other European Union Member State, which provide services in the Republic of Lithuania through agents, natural or legal persons.

"**Suspicious monetary operation or transaction**" shall mean a monetary operation or transaction related to an asset (including monetary funds) that, as may be suspected, may be directly or indirectly received from criminal activity or in the course of participation in such activity and (or), as may be suspected, may be associated with Money laundering and/or Terrorist financing.

"**Customer**" shall mean a person (usually a legal entity) performing monetary operations or concluding transactions with Transactive and therefore engaged in a Business relationship, in order to collect funds from consumers or distribute funds to consumers for business purposes (ie in exchange for goods and services).

"**Beneficial owner**" shall mean a natural person who owns or controls the Customer (a legal entity or a foreign company) and/or a natural person on whose behalf a transaction or activity is carried out.
The Beneficial owner shall mean:

(A) for a legal entity:

(a) a natural person who owns or controls, directly or indirectly, a legal entity through a sufficient share of that legal entity's stock or voting rights, including management through bearer shares, other than public limited companies or collective investment undertakings listed on regulated markets that are subject to requirements for disclosure of information about own business on a par with the European Union legislation or equivalent international standards, or who otherwise controls it. A natural person who holds 25 per cent or more or a stake of 25 per cent or more in the Customer's equity shall be considered the direct Beneficial owner. A natural person or persons who controls or control a company or a group of companies holding 25 per cent or more or a stake of 25 per cent or more in the Customer's equity shall be considered an indirect Beneficial owner(s);

(b) in a legal entity, which is being identified, a natural person in the senior executive position if there is no person who holds more 25 per cent or more of the company as specified in Clause (a) or if there is any doubt that the person who has been identified is the Beneficial owner;

(B) for a trust fund all of the following persons:
(a) the trustor(s);
(b) the trustee(s);
(c) the fiduciary(ies), if any;
(d) natural person(s) deriving benefit from a legal entity or an unincorporated entity or, if that person(s) is unknown, a group of persons whose interests that legal entity or unincorporated entity is supposed to represent or is acting on behalf of;
(e) any other natural person who actually controls the trust fund, available direct or indirect property, or other means;

(C) for a trust-like legal entity that administrates and allocates funds, a natural person who holds a position on a par with the position specified in Clause (B) above.

"Fictitious bank" (also known as a "shell bank") means a financial institution or an institution that carried out activities equivalent to those carried out by financial institutions, incorporated in a jurisdiction in which it has no physical presence nor any meaningful management, and which is unaffiliated with a regulated financial group.

"High-risk third countries" refers to those countries publicly identified by the European Commission and/or Financial Action Task Force as having strategic deficiencies in their national AML/CTF regimes that pose significant threats to the financial system of the European Union.

The firm must apply enhanced due diligence (EDD) measures to mitigate the risks arising from any Business relationship with a person established in a High-risk third country.

"**Individual risk assessment**" shall mean customer risk assessment related to individual Business relationship.

"**Monetary operation**" shall mean any payment, transfer or receipt of money..

"**Money laundering**" shall mean:

- the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
- the concealment or disguise of the true nature, origin, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;
- the acquisition, possession or use of property, knowing, at the time of receipt/transfer, that such property was derived from criminal activity or from an act of participation in such activity;
- preparation, attempts to commit and complicity in the commission of any of the activities mentioned above.

"**Politically exposed persons**" or "**PEPs**" shall means natural persons who are or have been entrusted in the preceding year with prominent public functions and Immediate family members or persons known to be Close associates of such persons. Prominent public functions shall mean the following functions in the Republic of Lithuania, EU, international or foreign state institutions:

(A) the Head of the State, the Head of the Government, a minister, a vice-minister or a deputy minister, the State Secretary, the Chancellor of the Parliament or the Government or a ministry;

(B) a member of the Parliament;

(C) a member on the Supreme Court, the Constitutional Court or any other judicial authority whose decisions are not subject to appeal;

(D) the mayor of a municipality, the head of a municipal administration;

(E) a member of the management body of the supreme national audit and control body or the chairman, deputy chairman, or member of the board of a central bank;

(F) an ambassador, a chargé d'affaires, commander of the Lithuanian armed forces, commanders of armed forces and units, Chief of Defense Staff or a high-ranking military officer of armed forces of a foreign state;

(G) a member of a managing or supervisory body of a state-controlled entity, public limited company, private limited company where the state owns a stock entitling it to more than ½ of all votes at a general meeting of shareholders of said entity or company;

(H) a member of a managing or supervisory body of a municipal entity, public limited company, private limited company where the municipality owns a stock entitling it to more than ½ of all votes at a general meeting of shareholders of said entity or company and which is considered a large company under the Company Law of the Republic of Lithuania;

(I) the head or deputy head or member of a managing or supervisory body of an international intergovernmental organisation;

(J) the head, deputy head, or member of a managing body of a political party.

"**Risk assessment**" shall mean Money laundering and/or Terrorist financing risk assessment, which is performed by Transactive in order to determine all Money laundering and/or Terrorist financing risks inherent to its business (by covering all business activities of Transactive).

"**Terrorist financing**" shall mean the provision or collection of funds, by any means, with the intention that they should be used (or in the knowledge that they are to be used) in full or in part, in order to carry out a terrorist offence.

"**Property**" shall mean things, securities, other financial instruments, other assets and interests, products of intellectual activity, information, actions and outcomes of actions, other property- and non-property-related valuables, as well as any other physical or not physical, movable or immovable, tangible or intangible property and documents or instruments of proof of title to such property or the related rights existing in whatever (including electronic and digital) form.

3 Policy Statement

It is the policy of Transactive to actively prevent the services of the firm being used to facilitate financial crime, Money laundering and/or Terrorist financing.

Strict compliance with all applicable regulations will also protect the shareholders, senior management and staff of the firm, as individuals, from the risks of breaches of law, regulations, and supervisory

requirements, and to preserve the reputation of Transactive against the damage that could be caused by being implicated in Money laundering and Terrorist financing activities.

To achieve these objectives, it is the policy of this firm that:

- every staff member shall meet their personal obligations as appropriate to their role and responsibilities;
- commercial considerations cannot take precedence over Transactive's anti-Money laundering commitment;
- the firm shall appoint a member of the Board, an Anti-Money Laundering Compliance Officer, and a deputy to cover in their absence, and they shall be afforded every assistance and cooperation by all members of staff in carrying out their duties and responsibilities.

Transactive will strictly comply with all applicable AML / CTF rules and regulations with specific emphasis on:

- a culture of compliance to be adopted and promulgated throughout the firm towards the prevention of financial crime;
- a commitment to ensuring that Customer's identities will be satisfactorily verified before the firm accepts them;
- a commitment to "knowing its Customer" appropriately - both at acceptance and throughout the Business relationship - through taking appropriate steps to verify the Customer's identity and business, and the reasons and purpose of their Business relationship with Transactive;
- a commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and to establishing procedures to implement these requirements; and
- recognition of the importance of staff promptly reporting their suspicions internally.

At the heart of our policies, procedures and controls, and consistent with FATF Recommendation 1, is the risk-based approach. The risk-based approach means that we focus our resources on the areas of greatest risk.

Our policies, procedures and internal controls are designed to ensure compliance with all applicable anti-Money laundering and anti-Terrorist financing regulations and regulatory guidelines and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

4 Corporate Governance

Corporate governance is the mechanisms, processes and relations by which corporations are controlled and directed. Governance structures and principles identify the distribution of rights and responsibilities among different parties within Transactive (such as the Board, managers, shareholders, staff members and other stakeholders) and include the rules and procedures for making decisions in corporate affairs. Corporate governance includes the processes through which Transactiuve's objectives are set and pursued in the context of the social, regulatory and market environment. Governance mechanisms may include monitoring the actions, policies, practices, and decisions of corporations, their agents, and

affected stakeholders. Corporate governance practices are affected by attempts to align the interests of stakeholders.

In terms of AML/CFT, Transactive is under a legal obligation to maintain, test and communicate internal control procedures for the purposes of detecting and preventing money laundering and the financing of terrorism.

The objective of corporate governance is to safeguard stakeholder's interest in conformity with public interest on a sustainable basis. Corporate Governance determines the allocation of authority and responsibilities by which the business and affairs of Transactive are carried out by its Board and senior management including how they:

- Set Transactive's strategy and objectives;
- Select and oversee personnel;
- Protect the interests of customers, meet shareholder obligations and take into account the interests of other recognised stakeholders;
- Align corporate culture, corporate activities and behaviour with the expectation that Transactive will operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations.

4.1 The Board

The Board has a critical oversight role - as the senior-most management of the company, they should approve and oversee policies for risk, risk management and compliance. The Board also should have a clear understanding of the ML risks, including timely, complete, and accurate information related to the risk assessment to make informed decisions. The Board as senior management takes responsibility for the identification, assessment and management of ML/TF risks. Along with the Director, the Board should appoint a qualified Chief Compliance Officer (the CCO) with overall responsibility for the AML/CTF function and provide this senior-level officer with sufficient authority that when issues are raised they get the appropriate attention from the Board, the Director and the business lines. The Board is responsible for the overall AML / CTF compliance policy of Transactive and ensuring adequate resources are provided for the implementation of proper controls to mitigate the risks, proper and constant training of staff and the implementing of risk systems. The Board will receive and consider annual compliance reports sent by the CCO. In the case of an increased risk of AMLTF or the disclosure of new circumstances affecting AMLTF risk management, the CCO shall notify the Board no later than within 5 days.

The Board is also authorised to make the following decisions at the request by the Chief Risk Officer of the Transactive Group (the CRO) or Chief Compliance Officer (the CCO):

- on starting a business relationship with applicants, that may possess high reputational or operational risk for the company,
- to enter into a business relationship with an applicant with whom it would not be possible to enter into business relationship due to previously resolutions adopted by the Board

- decision to allocate "Maksimum on account" limit that exceeds EUR 20 M.

4.2 The Onboarding Committee

The Onboarding Committee consists of the Managing Director, the Chief Business Officer and the Chief Risk Officer of of the Transactive Group (the CRO), as well as Chief Compliance Officer (the CCO). Other managers or invitees may participate in the Committee meetings.

The committee has two main functions:

(1) At the CCO's request, it makes decisions on starting a business relationship with particularly high-risk Customers at the CCO request.

(2) Decides, at the CCO's request, to enter into relationships with Customers requiring daily outbound or maximum on accounts limits of more than EUR 12 million.

4.3. Director (General Manager)

The Director will receive and consider the compliance reports sent by the CCO and authorize changes based on the recommendations if required. Director will also receive reports on particularly significant changes that may present risk to the organization. Assistance may be given to the CCO in the preparation of the AML/CTF program.

4.4. Compliance Department

The Compliance Department, led by the Chief Compliance Officer, reports directly to the Board, and is responsible for ensuring Transactive's compliance with all regulatory and legal papers.

The Department consist of three teams: the (i) MLRO team, led by the MLRO; (ii) ML/TF prevention team, led by Lead AML Officer, and (iii) Compliance and Legal team, led by Deputy CCO (this team is not directly involved in AML / CTF prevention, rather on Quality assurance / control functions).

4.4.1. Chief Compliance Officer (CCO)

The CCO (at his absence – her/his Deputy) acts as a first point of contact for all compliance issues for the Transactive staff. His/her responsibility is to prepare reports for consideration of the Board and conduct risk assessments of compliance systems, development and regular review of internal rules and guidelines.

The CCO must ensure that everyone is periodically informed of any changes in anti-Money laundering or anti-Terrorist financing legislation, policies, and procedures, as well as current developments and changes in Money laundering or Terrorist financing activity financing schemes particular to their jobs.

CCO approval is required to enter into business relationship with all High-risk applicants or to approve Customers' operational limits above EUR 2 Mio.

The CCO establishes and implements/updates the risk scoring matrix following regulatory guidance and for review and approval by the Board.

4.4.2. (Lead) AML Officer

The ML/TF prevention team, led by the Lead AML Officer, is responsible for proper assessment of all applications on onboarding stage, review of provided documents by the applicants, review of aplicant's legal representative's and identification and verification and individual risk assessment of all every new applications. Regular review of documents and updated information/data, submitted by the customers, and risk-reassessment of the clients is also under the team' responsibility.

The team reviews Customers identification information to ensure that all the necessary information and documentation has been obtained. AML Officer approval is needed to enter into business relationship with Low or Medium risk applicants.

He/she undertakes regular analysis of KYC documents' package provided by the Customers, including assessment of documentary evidence provided by Customers, and assists in making any necessary amendments to AML/CTF policy and manual in line with risk assessment.

AML Officer provides recommendations to the CCO to terminate business relationship with the Customers if the AML risk posed by the Customer to Transactive is above the risk appetite and/or Customer do not cooperate properly answering the additional questions, updating documents and information about his activities, legal representatives and business owners.

The AML Officer shall report to CCO on the status of received, rejected and under-review applications

4.4.3. Money Laundering Reporting Officer (MLRO)

The MLRO team, that is consisted by Fraud Investigation group and Transaction Monitoring Group, led by the MLRO, is responsible for transaction monitoring and transactions analysis and risk assessment, conducting fraud investigation cases), cooperation with law enforcement institutions as well as review and response to all requests and inquiries received from regulators, financial crime investigation authorities, clients, and 3rd parties. The team is also responsible for proper implementation of the sanctions framework to comply with the Sanctions Policy.

The MLRO is responsible for Transaction monitoring, receiving internal disclosures and making reports about suspicious transactions to the Financial Crime Investigation Service (FCIS) and Transactive's successful cooperation with FCIS.

The MLRO undertakes regular random analysis of transactions including assessment of documentary evidence provided by Customers and assists in making any necessary amendments to AML/CTF policy and manual in line with risk assessment. MLRO shall periodically, however at least once a year, report to the Board on performance of the functions assigned to him, by submitting the information in writing. MLRO shall report to the CCO on aggregate risk level of the Customer's portfolio as well as agreed risk parameters used to describe risk related to the customers.

MLRO provides recommendations to the CCO to terminate business relationship with the Customers if AML risk possessed by the Customer to Transactive is above risk appetite and/or Customer do not cooperate properly answering the additional questions about transactions on the accounts, providing and/or updating documents and information about his activities.

4.4.4. Staff

Other staff members are responsible familiarize with this Policy, other internal procedures related to their job role and understanding responsibilities. Ensure Transactive procedures are adhered to and obtaining all documentary evidence as outlined within the onboarding procedure. Ensure that all suspicious activity is reported to the MLRO or CCO as soon as possible via email and/or by any other method(s) specifically designed for that purpose.

All other staff members are responsible for knowing the AML/CTF Policy and understanding responsibilities.

5 The Compliance Programme

5.1 The CCO

Transactive has appointed a CCO who will also perform functions with relation to AML/CTF with full responsibility for Transactive's anti-Money laundering compliance.

The CCO:

- will manage the Compliance Department,
- will monitor the day-to-day operation of Transactive's AML/CTF policies and respond to any reasonable request made by the Bank of Lithuania, the FCIS or other law enforcement bodies, if any;
- has the authority to act independently in carrying out their responsibilities, which includes direct access to the Bank of Lithuania and appropriate law enforcement agencies, in order that any suspicious activity may be reported to the right body as soon as is practicable and in terms required by law;
- has the authority and the resources necessary to discharge his/her responsibilities effectively;
- is from a senior level and has direct access to senior management and the Management Board ;
- may choose to delegate certain duties to other employees, but wherever such a delegation is made, the CCO retains ultimate responsibility for the implementation of the compliance regime within the firm;
- at least monthly the CCO will issue a report (the CCO Monthly Report) to the senior management of Transactive on the operation and effectiveness of the Money laundering controls. This report shall cover improvements, remedial programmes, the outcome of any internal audit reviews of the AML/CTF processes, and other relevant items.

Deputy CCO replaces CCO during his absence.

Deputy CCO:

- assists and supports CCO leading, managing and building an Compliance team;
- ensures consistency and compliance with the regulatory policies and internal controls of the Company's activities;

- improves an anti-money laundering and terrorist financing framework and ensure full compliance with AML provisions applicable to the Company;
- organises / attends meetings and training in the field of Compliance within the Transactive group of companies;
- oversee and ensure that overall AML risk is aligned toCompany's business objectives, products and processes;
- conducts quality ensurance (compliance control) function;
- ensures that the AML risk assessment is carried out across all licensed activities, routinely reviewed and updated accordingly;
- carry out reports to the Bank of Lithuania and to maintain a direct and engaged relationship with the Bank of Lithuania;
- is involved in preparation CCO reports to the Board.

5.2 Compliance Policies and Procedures

Transactive has policies and procedures to assess the risks related to Money laundering and Terrorist financing. These policies and procedures are:

- written and maintained by the CCO or third parties (Walless Law Company);
- approved by the Board;
- communicated, understood and adhered to by everyone dealing with Customers or their transactions, including those who work in the areas relating to Customer identification, record keeping, and reportable transactions, who need enough information to process and complete a transaction properly as well as to ascertain the identity of Customers and keep records as required;
- policies and procedures which incorporate the reporting, record keeping, Customer identification, risk assessment and risk mitigation requirements applicable.

Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff and Transactive itself.

5.3 Company Risk Assessment

Transactive will analyse potential threats and vulnerabilities related to Money laundering and Terrorist financing to which the business is exposed to and will provide such analysis and its results in a company wide risk assessment documentation.

Company-wide risk assessment shall be performed using the firm's methodology approved by the Board which shall cover at least the following:

- sources used for the performance of the company-wide risk assessment;
- procedure for data collection and assessment;

- indicators indicating risk of Money laundering and Terrorist financing, its likelihood and impact;
- responsibilities and liability of the employee, carrying out the company-wide risk assessment;
- procedure for provision of information to the management bodies of the firm with respect to the carried out company-wide risk assessment;
- the frequency and procedure for reviewing and updating the company-wide risk assessment;
- procedure for drawing up and implementing action plan for risk management (mitigation) measures to be applied in the firm.

The risk assessment will document and consider the following:

- Product, service, transaction and service delivery channels risk;
- Country, Geographic locations and areas of operation risk;
- Customers, Business relationships and underlying Beneficial owners risk.

The risk assessment may identify high-risk situations for which risk mitigation controls and monitoring may be required. The risk assessment is not static and will change over time.

The risk assessment will be documented, reviewed and updated on a regular basis (which will be at least annually) and when significant changes occur and will be proportionate to the scale, nature and services conducted by Transactive. The Board and risk committee will be informed about all risk assessment results. If the results are that current measures are inadequate then a plan will be put in place to enhance or implement mitigation measures.

The risk assessment will identify and document the level of risk in details (through the use of statistical information as required). Such statistical information could include the number of Customers who are high risk/very high risk, and the number and value of high risk payment transactions. Any internal or external sources of data will be clearly referenced.

Any new product or service should also include a risk assessment prior to being launched. If existing products or services are launched to a new Customer segment, in a new Geographic location or through new product or service delivery channel, the risk of Money laundering and Terrorist financing related to the aforementioned factors shall be assessed by Compliance team.

5.3.1 Customer and Business Risk

5.3.1.1 Products, Services and Delivery Channels

Transactive will identify products and services or combinations of them that may pose an elevated risk of Money laundering or Terrorist financing. Products and services that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk. Certain services have also been identified by financial regulators, governmental authorities or other credible sources as being potentially high-risk for Money laundering or Terrorist financing, for example:

- wire transactions;
- transactions involving third parties;
- new product requests;
- non-face-to-face services and operations.

5.3.1.2 Country, Geographic Locations and Areas of Operation

Certain geographic locations potentially pose an elevated risk for Money laundering and Terrorist financing. These have been described by the FATF and by other resources such as Transparency International.

Customers from, or doing business in, these countries will be regarded as high risk or prohibited:

- any country subject to sanctions, embargoes, or similar measures;
- any country indentifed as a high-risk third country by the European Commission;
- any country identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;
- any country known to be a tax haven, source of narcotics or other significant criminal activity;
- any country identified by the FATF as non-cooperative in the fight against Money laundering or Terrorist financing or subject to a FATF statement;
- any country identified by credible sources as lacking appropriate Money laundering or Terrorist financing laws and regulations, or as having significant levels of corruption and/or predicate offences to Money laundering;
- any country without adequate capacity of the legal and judicial system effectively to prosecute offences with relation to corruption and Money laundering;
- any country without effective AML/CTF supervision.

Transactive does not do business with or provide services to anyone in any country belonging to a list of select countries subject to comprehensive international sanctions (the “Sanctions List”).

Generally Transactive does not do business with or provide services to anyone in any country listed as a “high-risk third country” by the European Commission and any such business would be subject to the additional enhanced due diligence (EDD) requirements as established by law.

5.3.1.3 Customers and Business Relationships, and Underlying Beneficial owners

The risk assessment requires that we know our Customers and the nature of their business. This is not limited to identification or record keeping, but it is also about understanding our Customers, including their activities, transaction patterns, and how they operate. Consequently, Transactive performs invidual risk assessment (as further described herein). Examples of the factors that will be considered are:

- how long we have known the Customer and had a Business relationship;
- what is Customer’s business and products/services used;
- Customers wanting to carry out large transactions;
- Customers with regulatory or enforcement issues;
- Customers with multiple online complaints;
- businesses that are cash intensive;
- Customers whose identification is difficult to check;
- Customers whose principals/legal representatives and/or UBO include Politically exposed persons;
- the Business relationship is conducted in unusual circumstances;
- legal persons or arrangements that are personal asset holding vehicles;

- companies that have nominee shareholders (other than where they are subsidiaries of suitably regulated financial institution) or shares in bearer form;
- the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

Customers involved in the following business sectors or activities would be regarded as exposing themselves and Transactive to higher risk:

- oil,
- guns,
- precious metals,
- tobacco products,
- cultural artefacts and other assets that are valuable from the archaeological, historical, cultural or religious point of view,
- items of rare scientific value,
- dealing with ivory and protected species;

5.3.2 Regulatory risk

Regulatory risk means not meeting our obligations under the Lithuanian AML/CTF regulatory regime. Examples (a non-exhaustive list) of breaches of regulatory obligations include:

- Customer identification not done properly;
- failure to train staff adequately;
- not having an (effective) AML/CTF programme and/or procedures;
- failure to report suspicious transactions;
- not having a CCO;
- failing to keep complete Customer records;

5.3.3 Risk Matrix and Individual Risk Assessment

When a Customer is identified as high-risk, they are subject to more frequent ongoing monitoring and updating of Customer identification information, as well as any other appropriate enhanced measures.

For new Customers, Transactive shall perform an individual risk assessment at the beginning of a Customer relationship and for existing Customers on an ongoing basis.

For ongoing monitoring, all Customers are classified with a risk tier. The risk tier can be offset by a lower or higher risk factor in certain circumstances:

- Customers will initially be given the highest risk category they fall under through a review of:
    - business types;
    - products and services;
    - geographic location;
    - payment types;
- The CCO will define high risk business types, geographic locations and payment types and risk thresholds following regulatory guidance as well as taking into consideration company-wide risk

assessment results, and will report the risk rules to the Board for approval. Some of the risk factors increasing and decreasing Money laundering and/or Terrorist financing risk are also indicated in The Risk Factors Guidelines as prepared and published by the Joint Committee of the European Supervisory Authorities.

- High risk status due to being a PEP cannot be offset if the connected person is still a PEP. Geographic location risk tiers cannot be offset except under special circumstances.
- The ongoing monitoring may give rise to factors which will allow an amendment of the risk tier of a merchant.
- Certain merchants are given restricted status where they require a regulatory licensing or special boarding conditions to be taken on as a Customer. Restricted status is not primarily an AML/CTF risk category.

Restricted status cannot be offset, but for clarity, a "restricted status" merchant is not necessarily a high-risk merchant.

- High risk status applies to *inter alia* PEPs, non-face-to-face relationships or transactions without certain safeguards, certain business categories, certain geographic locations and certain types of payment. High risk status applies to other factors (e.g. certain distribution channels) as established by CCO.
- Moderate risk status applies to certain business categories and geographic locations.
- Generally, countries which are EEA members, will be classified as of lower geographic risk.
- When relevant information is received which may potentially influence the results of individual risk assessment, e.g. change in Customer and Beneficial owner identification data; receipt of certain information with respect to the Customer or its business; the Customer requires new service or product; the nature of Customer's Monetary operations and/or transactions change; the Customer's Monetary operations and/or transactions are suspious, or any other trigger event occurs, the individual risk assessment shall be reviewed and renewed, as needed.
- When results of individual risk assessment indicate that the Customer is assigned to a higher risk category, the firm shall require additional information, perform EDD or apply other risk management (mitigating) measures as decided by the CCO.
- There will be an annual review of the risk scoring by senior management and the CCO to determine ongoing risk policy and an enterprise risk assessment.

5.4 Compliance Training

Transactive has a training program for all employees and other individuals who act on behalf of Transactive to make sure that those who have contact with Customers, who see Customer transaction activity or who handle cash in any way understands the reporting, Customer identification and record keeping requirements.

All new employees of Transactive are required to complete anti-Money laundering and anti-Terrorist financing compliance training within their induction training period when they first join the firm. All employees will also be enrolled and undertake the comprehensive and regular firm-wide anti-Money laundering and counter-Terrorist financing training within their first six months of employment with the

exception applicable to the employees who are directly involved in application of the AML/CTF measures (such as the CCO) who must be introduced to the procedures of Transactive before they will start performing functions with relation to AML / CTF.

Training is currently conducted through an internal customised course and Transactive also makes use of publicly available courses and material, and purchased courses and materials particularly in certain specialist areas. The training program will be in writing but can be delivered electronically (via email and online forms) or by other means. The training program will be reviewed and updated by the CCO to reflect requirements. Currently the compliance training includes a main training course with a test which everyone must complete.

To ensure employee training is kept up to date, all existing employees will receive follow up training on new and existing AML / CTF and regulatory on a regular basis (at least within one year of their last training). If the online training test results show that a staff member does not understand the training material, Transactive will ensure that the staff member receives specialised one-on-one training to understand the AML / CTF material.

An employee log of assigned and completed training materials shall be kept up to date by the CCO and on file for five years (e.g. extract or download of training logs).

Relevant compliance training is for all employees and relevant service providers. This includes those persons in sales and in senior management and others who have responsibilities under the compliance regime, such as information technology and other staff responsible for designing and implementing electronic or manual internal controls. The CCO will review functions and arrange to provide suitable and customised training.

Our training will include at a minimum:

- an understanding of the reporting, Customer identification and record keeping requirements as well as penalties for not meeting those requirements;
- making all employees aware of the internal policies and procedures for deterring and detecting Money laundering and Terrorist financing that are associated with their jobs;
- delivering to employees and suppliers a clear understanding of their responsibilities under these policies and procedures;
- all those who have contact with Customers, who see Customer transaction activity, who handle cash or funds in any way or who are responsible for implementing or overseeing the compliance regime must understand the reporting, Customer identification and record keeping requirements.
- making all employees and agents aware of how Transactive is vulnerable to abuse by criminals laundering the proceeds of crime or by terrorists financing their activities;
- making all employees and agents aware that they cannot disclose that they have made a suspicious transaction report, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether it has started or not;
- that all employees and agents understanding that no criminal or civil proceedings may be brought against them for making a report in good faith;
- background information on Money laundering so everyone who needs to can understand what Money laundering is, why criminals choose to launder money and how the process usually works;

- details of what Terrorist financing is and how that process usually works.

The CCO is responsible for ensuring that everyone is periodically informed of changes in AML / CTF legislation, policies and procedures, and current developments in Money laundering or terrorist activity financing schemes particularly relevant to their jobs.

Certain employees, such as those in compliance, Customer services and operations, require types of specialised additional training which will be provided either through external services or internally. The training program will be reviewed and updated to reflect requirements.

6 Customer Identification and Due Diligence

Transactive will identify and verify Customers before transactions are conducted and prior to entering a Business relationship.

6.1 Customer Acceptance and Approval

Transactive enters into Business relationships with commercial organisations. These are usually merchants in certain areas which Transactive has targeted or has experience with. Transactive can take on multiple types of business but is selective. Not all merchant types or business methods are acceptable and Transactive maintains a list of unacceptable business types ("the Prohibited List"). Transactive also maintains a list of countries with which it will not do business. In addition, Transactive has lists of high risk business types, and countries and services which are not prohibited but are viewed with concern. These are business types or jurisdictions which have been identified by a number of sources as having a higher than average risk of Money laundering or Terrorist financing activity, and also of fraud and high charge back activity, and where the benefit of taking on a Customer is or may be outweighed by the higher risk of illegal activity.

6.2 Customer Identification

Transactive must apply Customer due diligence, which includes Customer identification, when:

1) establishing a Business relationship;
2) when there are doubts about the veracity of authenticity of previously obtained Customer or Beneficial ownership identification data;
3) in any other case where there are suspicions that the act of Money laundering and/or Terrorist financing is, was or will be performed.

Transactive enters into ongoing Business relationships with all Customers (there are no "one-off Customers") and therefore conducts Customer due diligence on all Customers.

Transactive will take all relevant, targeted and proportionate measures in order to establish whether the Customer operates on their own behalf or are controlled by others and to establish the Beneficial owner.

Transactive will not conduct transactions for any Customer who refuses or otherwise fails to submit data confirming their identity, or if the data submitted is incorrect, or they conceal the identity of the Beneficial owner, or they avoid submitting the data required, or the data submitted is insufficient.

Whenever Transactive identifies a Customer and the Beneficial owner, Transactive will also obtain from the Customer documents (where relevant) and information in order to understand the purpose and intended nature of the Customer's Business relationships as well as management, ownership and control structure of the Customer that is a legal person.

Identification of the Customer and the Beneficial owner is on the basis of documents, data or information obtained from a reliable and independent source.

Once a Business relationship is established Transactive must perform ongoing monitoring of the Customer's Business relationships, including scrutiny of transactions undertaken throughout the course of such relationship, to ensure that the transactions being conducted are consistent with Transactive knowledge of the Customer, the business and risk profile, including, where necessary, the source of funds.

The records and data on the identity of the Customer and the Beneficial owner must be regularly reviewed and kept up-to-date.

Customer identification measures shall be also applied when there is an obligation to submit information under Section 2 of Government Resolution No 1017 of 23 September 2015 regarding the Council Directive No 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (OJ 2011 L 64, p. 1) and the implementation of international treaties and agreements on automatic exchange of information on financial accounts of the Republic of Lithuania.

Transactive will not conduct transactions or establish Business relationships when they are unable to complete full due diligence and identification of a Customer. In any such case a notification to the FCIS is required.

Customer Identification is intended to confirm the existence and identify the organisations with which Transactive has a Business relationship; as well as obtain identifying information on Beneficial owners, signing authorities, and authorised employees of those organisations. This includes measures to:

- confirm the existence of the commercial organisation through identification documents;
- determine the individuals who control or act on behalf of the business and obtain identification information and documents as required, and verification of that information;
- establish the ownership, control and structure of the business and take reasonable measures to confirm the accuracy of the information obtained;
- record the purpose and intended nature of the Business relationship;
- conduct due diligence into the identities, type of business, business practices of the Customer including:
    - cross-referencing their names against government watch/sanction lists;
    - determining whether any of the individuals associated with the Customer are Politically exposed persons;
    - determining whether any third parties are involved;
    - reviewing their marketing material, including websites, and obtaining samples of their product;
    - reviewing their background, reputation and return rates;
- Keep records of all information and documents obtained.

Once the Customer's information has been collected, a review will be made by the Onboarding Team employee to ensure that all the necessary information has been obtained. In athypical cases/legal documents and or ownership structure or business activities information consultation of CCO (Deputy CCO) is mandatory.

Payment Officer , after a decision to enter into business relationship is given, must ensure that:

1) New IBAN account can be generated for onboarded Customer after successful KYC/Onboarding process and Customer acceptance;
2) no transactions can be carried out through bank accounts before applicant/ne customer will be accepted .

Transactive do not open and provide service for anonymous accounts.

Onboarding team/other responsible persons do not accpet new applicant/new Customer till any suspictions/concerns regarding documents, information, activity exists.

Detailed requirements for KYC documents/information and process of new client identification and verification is regulated in "On-boarding Procedure".

6.3 Simplified Customer Due Diligence

If the Money laundering or Terrorist financing risk is found to be low, a simplified due diligence (SDD) may be applied in the following cases:

(A) for companies that have their securities admitted to regulated markets of one of or several European Union Member States, and other companies of foreign countries that have their securities traded on a regulated market and are subject to business disclosure requirements as per European Union regulations;

(B) for state and municipality institutions;

(C) for the Customer, if the Customer is a financial institution governed by the provisions of the Law or a financial institution incorporated in another European Union Member State that has requirements on a par with the requirements of the Law in place, which is subject to supervision by the authorities for compliance with such requirements, also if international organisations have identified a low level of corruption in the country.

In applying a SDD for companies that have their securities admitted to regulated markets and for state ad municipality institutions , Transactive, for the purposes of Customer and Beneficial owner identification, deviate from the usual identity verification procedure and shall only:

(A) for the Customer (a legal entity) obtain the name, legal form, domicile (address), business address, code (if any) of the Customer (a legal entity);

(B) make sure that the Customer's first payment is made from the account with a credit institution, when the credit institution is registered in a European Union Member State or a third country that

enforces requirements on a par with those imposed by the Law and is subject to authority supervision for compliance thereto.

At the current stage, Transactive do not apply simplified Customer due dilliguence measures.

6.4 Enhanced Customer Due Diligence (EDD)

EDD shall be conducted through application of additional Customer and Beneficial owner identification measures.

Transactive shall always focus on any particular Money laundering and Terrorist financing threats that may arise by virtue of usage of products of any nature, other results of human labour, services, or transactions, when efforts are made to conceal the identity of the Customer or Beneficial owner (leaning towards anonymity), as well as by virtue of Business relationship or transactions with the Customer who was not identified with the Customer being present in person, and shall take immediate action to prevent the Property from being used for Money laundering and Terrorist financing purposes.

EDD shall be conducted under the following circumstances:

(A) when international Correspondent relationship with third country financial institutions are being carried out;

(B) for transactions or Business relationship with PEPs;

(C) for transactions or Business relationship with natural persons residing or legal entities incorporated in High-risk third countries which are identified by the European Commission as High-risk third countries;

(D) for transactions or Business relationship with legal entities incorporated in jurisdictions which are identified as High-risk third countries on the lists of jurisdictions having serious deficiencies in their AML regimes drawn up by the FATF;

(E) if individual risk assessment and management procedures point to a higher Money laundering and Terrorist financing risk.

In the course of international Correspondent relationship with third country financial institutions, Transactive shall:

(A) collect enough information about the correspondent institution to be able to appropriately understand the nature of its business and determine the reputation and quality of supervision of such institution from the publicly available information;
(B) evaluate the ML / TF prevention control mechanisms of the financial institution that receive the funds;
(C) obtain the consent of a senior executive (e.g. CEO, executive member of the Board, or CCO to enter into a Business relationship with such Customers;
(D) justify by documents the relevant obligations of each financial institution;

(E) ascertain itself that the correspondent institution has appropriately conducted a Customer identification procedure (including identification of the Customer with direct access to the correspondent accounts and other actions of the Customer's identification) and, if necessary, upon request of the correspondent institution, may provide appropriate data for the purposes of Customer identification;

(F) do not enter into or continue Correspondent relationship or another relationship with a Fictitious bank or a bank that is known to allow Fictitious banks to use its accounts. Transactive takes measures to make sure that financial institutions, which receive the funds, do not allow Fictitious banks to use their accounts.

In conducting Customer identification for transactions and Business relationship with PEPs, Transactive shall:

(A) establish and enforce internal procedures to determine whether the Customer, representative of the Customer and the Beneficial owner is a PEP;

(B) obtain the consent of a senior executive (e.g. CEO, executive member of the Board, or CCO) to enter into a Business relationship with such Customers or to continue Business relationship with Customers when they become PEPs;

(C) apply appropriate measures to identify the source of the Property and funds relating to Business relationship or a transaction;

(D) exercise enhanced monitoring of Business relationship.

In applying an EDD for natural persons residing or legal entities incorporated in High-risk third countries listed as such by the European Commission, Transactive shall follow the procedure outlined below and shall apply the following identification measures to mitigate the risks as they arise:

(A) obtain the consent of a senior executive (e.g. CEO, executive member of the Board, or Compliance Officer) to enter into or continue Business relationship with such Customers;

(B) additional information with respect to the Customer and Beneficial owner(s) allowing to assess the type of the Customer, its activities, link with high-risk countries;

(C) obtain additional information with respect to the nature of the intended Business relationship;

(D) obtain additional information on the source of the Customer's Property and funds;

(E) obtain information on causes of anticipated or executed transactions;

(F) enforce enhanced ongoing monitoring of the Business relationship with such Customers by increasing the number and periodicity of the control procedures and by selecting the types of transactions that will require further investigation;

(G) in case the Customer is opening an account, to make sure that the Customer's first payment is made from their account with a credit institution, when the credit institution is registered in a

European Union Member State, or in the home country of any other Transactive company, or a third country that enforces requirements on a par with those imposed by the Law and is subject to authority supervision for compliance thereto.

In case the FCIS establishes additional risk mitigation measures as provided for in Article 14(4^2) of the Law, Transactive will comply with these measures as instructed in applicable laws.

When applying EDD for legal entities incorporated in High-risk third countries listed as such by the FATF, and when Transactive risk assessment and management procedure points to an increased Money laundering and Terrorist financing risk, Transactive shall follow the procedure outlined below and shall apply, at its own discretion, one or several Customer and Beneficial owner identification measures to mitigate the risks as they arise, and shall:

(A) obtain the consent of a senior executive (e.g. CEO, executive member of the Board, or CCO) to enter into or continue Business relationship with such Customers;

(B) apply appropriate measures to identify the source of the Property and funds relating to the Business relationship or transaction (e.g. collect information about source of funds (wealth) to finance Customer's business, such as financial statements and/or other relevant financial information, such as tax declarations, extracts from public registries or security depositories to confirm the ownership of real estate or financial assets, bank account statements or other eligible documents, if not available on public sources, also business contracts to prove business profile, agreements to provide availability of financial resources (loan, investment agreements, etc.), partnership agreement deeds, trust deeds / areements, etc.);

(C) enforce enhanced ongoing monitoring of the Business relationship with such Customers.

6.5 Customer Identification for Corporations and Other Entities

6.5.1 Corporations

Certain information about the entity should be obtained as a standard requirement. We will then assess the risk of Money laundering or Terrorist financing, based on the combination of factors outlined in our risk matrix and then decide the extent to which the identity of the entity should be verified, using reliable, independent source documents, data or information. We will require information in respect of some of the individuals behind or connected to the Customer for the purpose of being satisfied that we know who the "Beneficial owners" of the entity are.

As part of the standard evidence, we must know the individual Beneficial owners who own or control 25% or more of the Customer entity or is to be considered as beneficial otherwise, even where these interests are held indirectly. Information must be obtained on the nature and purpose of the Business relationship and anticipated size and volume of transactions.

We will obtain the following as standard in relation to corporate Customers:

(i) Legal name and any additional business or DBA names;
(ii) The address of the principal place of business, mailing address, local office or other physical location;

(iii) Legal form;
(iv) Incorporation number and place of incorporation;
(v) Date of formation or incorporation;
(vi) Name, personal code, date of birth (if personal code is not available), citizenship of the executive director[1] or equivalent[2];
(vii) Names of other directors;
(viii) Names of all authorised signatories (if the Customer is represented not by its Senior Manager)
(ix) Power of Attorney (if applicable);
(x) Name, personal code, date of birth (if personal code is not available), citizenship of all Beneficial owners.

Data indicated in items (i)-(iv) shall be collected by obtaining a commercial registry extract (attached with the Apostille / legalized if applicable) from the Customer. Transactive may obtain company data (data, information, documents) indicated in items (i)-(iv) directly from state informational systems or registries ("the registry data") and do not require the Customer to provide it itself only if the Customer validates the registry data by signature (including an advanced electronic signature or qualified electronic signature). Transactive is not obliged to require the Customer to validate the registry data by signature as specified above, if the registry data does not differ from the registry data previously validated by the Customer and if the registry data obtained is with respect to the executive officer of the Customer (legal entity), as well as when the registry data is obtained from the Population Register of the Republic of Lithuania.

In the case of trusts Transactive requires documents about:

a) the settlor;

b) the trustee;

c) the protector, if any;

d) the natural person deriving benefit from a legal entity or an entity without legal personality or, if such person is not yet identified, the group of persons in whose main interest the legal entity or an entity without legal personality is set up or operates;

e) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

We will also verify the identity of the corporate entity from:

- Either a search of the relevant company registry and BO register (if such register exist in the country of company's registration)

Or

[1] Executive director is a person or persons who have the right to act on behalf of the legal entity.
[2] Such information on executive director(s) shall be collected in case such person(s) is not an authorized representative, as further described in Section 6.6 herein.

- Confirmation of the company's listing on a regulated market, which are subject to disclosure requirements consistent with European Union legislation

Or

- A certified copy of the company's commercial registry extract, certificate of incorporation or equivalent (attached with Apostille / legalized if applicable)

This standard evidence is likely to be sufficient to verify the identity of most corporate Customers. If, however, any of the circumstances outlined in our risk matrix exist then we may require additional information to be provided to be satisfied as to the Customer's identity. Detailed document / information requirements are also provided in the Onboarding Documentation Requirements Table of Transactive.

6.5.2 Other Entities

Further guidance on verifying the identity of a range of non-personal entities will be provided in internal guidance and procedures.

If any of these types of organisation wish to use our service please refer to the CCO.

6.6 Identifying Information for Authorised Users

Transactive's Customers are corporate entities (including partnerships and limited liability companies). In all cases, as well as confirming the existence of the corporate entity we will need to establish the identity of certain individuals who are authorised to represent the company.

This section sets out the standard identification requirements for individuals who are authorised representatives of corporate entities which have entered a Business relationship with Transactive. This is likely to be sufficient for most situations. If, however, the Customer is assessed as presenting a higher Money laundering or Terrorist financing risk, in line with our identified risk matrix, then we require additional identity information to be provided and increase the level or verification accordingly.

Where the result of the standard verification check gives rise to concern or uncertainty over identity, the number of matches that will be required to be reasonably satisfied as to the individual's identity will increase. Any concerns must be notified to the CCO (Deputy CCO).

Staff may also need to follow this guidance when identifying, and verifying the identity of Beneficial owners, directors and authorised signatories and any other relevant individuals associated with the relationship or the transaction. Any issues relating to Beneficial owners of high and very high risk cathegory customers should be raised with the CCO (Deputy CCO).

If Customer is unable to produce a primary ID, the reasons for this should be noted and they may not be able to open an account.

All documentary evidence must be recent, i.e. not older than 3 months.

ID Documents, e.g. passport, ID card (only for the EEA / UK citizens) , drivers license (for the EEA/UK residents, only with a signature), permanent residency permit must be valid and not expired.

INDIVIDUAL IDENTIFICATION REQUIREMENTS (FACE-TO-FACE AND LOW-RISK)

Type	Information Required	Documents Required
Directors	-Names, personal codes, dates of birth (if personal code is not available), residential addresses*, and occupations, citizenship of all Directors -Names of all Directors	• A Photo of ID document (with proof of identity, signature (if required in the document) and personal code or date of birth)
Authorised Signatories	-Names, personal codes, dates of birth (if personal code is not available), residential addresses*, of signatories (with authority over transactions) identified through documents - Power of Attorney	All relevant authorised signatories will require items of documentary identification: • A Photo of ID document (with proof of identity, signature (if required in the document) and personal code or date of birth)
Beneficial owners (25% or over of shares)	-Legal Name, Address*, Unique Identification number, -Further information may be required on owners on a risk-based approach.	• We may require documentary identification of owners on a risk- based approach • The following information on the ultimate Beneficial owners (individuals) also need to be collected: name, surname, personal code or date of birth (if personal code is not available), citizenship as well as public sources where the identity of the individual may be verified

INDIVIDUAL IDENTIFICATION REQUIREMENTS (NON-FACE-TO-FACE OR HIGH-RISK AND VERY HIGH RISK)

Type	Information Required	Documents Required
Directors	-Names, personal codes, dates of birth (if personal code is not available), residential addresses*, and occupations, citizenship of all Directors -Names of all Directors	• A Photo ID document (with proof of identity, signature (if required in the document) and personal code or date of birth and citizenship) •
Authorised Signatories	-Names, personal codes, dates of birth (if personal code is not available), residential addresses*, of signatories (with authority over transactions) identified through documents - Power of Attorney	All relevant authorised signatories will require items of documentary identification: A Photo ID document (with proof of identity, signature (if required in the document) and personal code or date of birth and citizenship)
Beneficial owners (25% or over of shares)	-Legal Name, Address*, Unique Identification number, -Further information may be required on owners on a risk-based approach.	• We may require documentary identification of owners on a risk- based approach. • The following information on the ultimate Beneficial owners (individuals) also need to be collected: name, surname, personal code

		or date of birth (if personal code is not available), citizenship as well as public sources where the identity of the individual may be verified

**Please note P.O. boxes are not acceptable addresses.*

If citizenship is not required / missing in the identity document, the Customer shall be asked to provide this information additionally.

Transactive identifies Customers remotely using electronic media that allows live video transmission enabling capturing the image of the Customer representative's face and the original of the identity document of such representative. When identifying Customers remotely, Transactive complies with the Technical Requirements.

Transactive may also identify Customer by making sure that prior to provision of services to the Customer, the Customer's first payment is made from the account with a credit institution, when the credit institution is registered in a European Union Member State or a third country that enforces requirements on a par with those imposed by the Law and is subject to authority supervision for compliance thereto and by receiving a certified hard copy of a ID document of the Customer. When the identity of the representative (who is employee of the legal entity) of the Customer – legal entity is verified then the ID document may be certified by the authorized persons of such legal entity. In other cases, the ID document must be certified by notary public and attached with Apostilled or legalized.

When identifying the Customer remotely, the Customer shall submit all the data about the legal representative and Beneficial owner as provided in the table above. The data submitted by the Customer shall be validated by using electronic identification means allowing live video streaming, as defined in herein and in the Technical Requirements, or by signature on a written form document (notarized).

When identifying the Beneficial owner of Lithuanian legal entities, Transactive will additionally use the Legal Entities Information System (JADIS), where it shall obtain information on Beneficial owners of the Customer. Transactive may use other information systems, as well as registers where the data on participants of legal entities is stored.

Transactive, having determined that information submitted by the Customer-Lithuanian Legal entity with respect to its Beneficial owners does not correspond to the information obtained from JADIS, shall notify the Customer and suggest to provide relevant information to JADIS.

For the purposes of Regulation EC 2015/847 on information accompanying transfers of funds (commonly known as the Payments Regulation or the Wire Transfer Regulations), we allocate each Customer with an account number. This number will be sent with the Customer's name (as well as other information required by the said regulation) to comply with the regulation.

In terms of beneficial ownership, we will ask every Customer whether they are acting in their own capacity or on behalf of another person. If they are acting for another person then we will require details of such. Detailed document / information requirements are also provided in the Onboarding Documentation Requirements Table of Transactive.

Sources of evidence

Proof of Identity - Acceptable photo identity:

- Original of valid passport; or
- Original of national identity card, or;
- Driver license issued in a State of the EEA meeting the requirements laid down inAnnex I of Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licences (recast) a driving licence, or
- Lithuanian Residency Permit.

When accepting evidence of identity from a Customer, it is important that we make sufficient checks on the evidence provided to satisfy us of the Customer's identity, and that we keep a record of the checks made. This will be done by employees of Compliance department (Onboarding Team)

Usual checks on photo ID may include:

Visual likeness against the Customer

- Does the date of birth on the evidence match the apparent age of the Customer?
- Is the ID valid?
- Is the spelling of names the same as other documents provided by the Customer?

Checks on secondary evidence of ID may include:

- Does the name of the Customer match with the name on the photo ID?

Where the Customer is not physically present for identification purposes we must obtain further evidence of identity and it's verification in line with our stated policy and requirements laid in this Document and using remote identification service (UAB "Ondato").

Identification documents will be obtained before the authorisation of any transactions in the Business relationship. Identification includes verifying the Customer's – legal entity's corporation's existence, their name, and address, and establishing their ownership, control and structure. This means confirming who their directors are and their beneficial ownership.

Documents which can confirm existence include certificates of incorporation, memoranda and articles of association, partnership agreements, and articles of organisation or any other similar record. If electronic versions of these records are obtained they will be from an official source.

If the registered legal entity has been in existence for over a year we will also need to confirm that it still exists and is active. To do this we will refer to an official government registry or service. If this is not available we will require a certificate of good standing or an equivalent recent document issued within the last year.

Copies will be kept of all the documents used for identification.

Reliance on the third parties

Third parties are financial institutions or other obliged entities (including official Agents of Transactive registered in the Registry of Bank of Lithuania) registered in a European Union state or UK or other state who are subject to mandatory professional registration, who apply due diligence and record keeping requirements in respect of Customers and Beneficial owners equivalent to EU Money laundering requirements and is supervised by competent authorities for compliance thereof (so if situated in a Non-EU country that country would have to have requirements equivalent to EU requirements – a list of such countries will be available from the CCO and who are supervised by competent authorities for compliance with such requirements).

Transactve may use third party information about a customer or a beneficiary to identify a customer or a beneficiary, provided that it has sufficient means to ensure that the third party voluntarily complies with both of the following conditions:

1) upon request, immediately provide the requesting Transactive with all the requested information and data that are required to have in compliance with the customer or beneficiary identification requirements;

2) upon request, immediately provide Transactive with copies of documents related to the identification of the customer or beneficiary and other documents related to the customer or beneficiary that are required to be in compliance with the customer or beneficiary identification requirements.

A co-operation agreement may be signed with a third party if it meets requirements stated in this Document after the analysis of the third party's AML Policy/documention and procedures and if third party satisfy the customer identification, data protection requirements, has qualified staff/officers responsible for AML (if third party is official Agent of Transactive – after registering on Bank of Lithuania Registry)requiremenr.

After signing cooperation agreement with third party such Transactive partner can be called/have status of referral for new clients attracting.

6.7 Mitigation of impersonation risk

Where identity of Customer's representative is verified electronically, Transactive will apply an additional verification check to manage the risk of impersonation fraud. The standard check will be conducted using electronic media that allows live video transmission which enables capturing the image of the Customer representative's face and the original of the identity document as produced by the Customer.

6.8 Beneficial ownership and Control

When we identify a Customer, we will obtain, take reasonable measures to confirm, and keep records of, the information about an entity's shareholders, the entity's directors, and on the ownership, control, and structure of the corporation.

Beneficial owners are the individuals who ultimately control the corporation or entity (and so cannot be another corporation or entity) and include all the individuals who directly or indirectly own or control 25 per cent or more of the corporation's shares (please see the definition of "Beneficial owner" provided in this manual for further details).

Here, reasonable measures would include asking the Customer to provide documentation. While we can rely on the information provided by Customers we need to assess whether the documentation is appropriate.

In most cases, Beneficial ownership information can be obtained through documents such as articles of incorporation or constitution, annual returns, shareholder or partnership agreements, trust deeds and records of decisions. Determining the Beneficial owner means searching through as many levels of information as necessary.

There may also be cases where there is no individual who owns or controls 25% or more of an entity. These still require a record of the measures taken and the information obtained in order to reach that conclusion.

If this information cannot be obtained or its accuracy cannot be confirmed, we need to identify the senior officer of the corporation or other entity; and treat that corporation or other entity as high-risk. Furthermore, Transactive shall save all related identification documents and information, including any difficulties that have arisen during the process.

6.9 Keeping Customer Identification Information Up to Date

Once the identity of a Customer has been confirmed, it does not have to be confirmed again. But if there is any doubt about the information held, then that identification will be obtained again, including the identification of individuals representing the Customer.

Transactive has a program of reviewing the documentation on existing Customers and then updating that documentation as appropriate. Any changes to identification such as a change of name require an official certificate or an appropriate corporate registry extract. Any addition of authorised individuals to an account will require identification as per the Customer identification requirements.

If an individual has been identified already in relation to another Customer then that individual does not have to be identified again.

Reasonable measures will be taken to keep Customer identification information, including beneficial ownership and Business relationship information, up to date.

Measures to keep Customer identification information up to date include asking the Customer to provide information to confirm or update identification information, and consulting a paper or electronic record.

6.9 Politically Exposed Person Determination

At account opening Transactive will determine whether a Customer relationship involves a Politically exposed person (PEP). If the Customer, its representativeor a Beneficial owner, is a PEP the account will be referred to senior management prior to entering into an ongoing service agreement with the account applicant.

A PEP Questionnaire is included in the account application form and all names will be searched through credible sources of commercially or publicly available information.

Confirmed PEPs will be high risk, subject to EDD, and no account will be opened or large transaction proceeded without the express authority of the managing director.

PEPs are defined as “an individual who is or has, at any time in the preceding year, been entrusted with Prominent public functions and an Immediate family member, or a known Close associate, of such a person”.

PEP status itself does not, incriminate individuals or entities. It does, however, put the Customer, its representative or the Beneficial owner, into a higher risk category (High od very High).

PEPs do not automatically lose “high risk” status if they are no longer holding public office. They remain “high risk” requiring EDD for at least one year and after that Transactive will apply a risk-based approach to determine whether a former PEP should still be classified as high risk.When deciding whether a person is a known Close associate of a PEP, the firm need only have regard to any information which is in their possession, or which is publicly known.

Transactive will have

- appropriate risk-based procedures to determine whether a Customer, Customer’s representative, Director or Beneficial owner is a PEP;
- obtain appropriate senior management (CEO, executive Board member or Compliance Officer) approval for establishing a Business relationship with such a Customer;
- take adequate measures to establish the source of wealth and source of funds which are involved in the Business relationship or occasional transaction; and
- conduct enhanced ongoing monitoring of the Business relationship.

7 Record Keeping

Transactive will keep records of Customer due diligence and transactions.

7.1 Logs

Transactive shall keep the following logs of:

(A) reports submitted to the FCIS and of suspicious operations or transactions;

(B) the following Monetary operations carried out by the Customer:

(a) one-time or related operations or entering in transactions in the amount of EUR 15,000 or more, or equivalent in a foreign language, regardless of whether the transaction is being performed within the scope of one operation or related operations;

(b) money transfers, carried out in accordance with Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

(C) Customers with which transactions or the Business relationship have been terminated under the circumstances related to infringements of the procedure for the prevention of Money laundering and Terrorist financing.

Transactive must enter the following information in the logs specified in Item (B) above:

(A) data verifying the identity of the Customer or a representative thereof (where the Monetary operation or transaction is carried out through a representative) (for a natural person – given name and last name, date of birth, personal identification number or another unique sequence of symbols assigned to the person for identification purposes, citizenship; for a legal entity – name, legal form, registered office, code (if any has been assigned);

(B) information about the Monetary operation or transaction: the date of performance of the transaction, the description of the Property in respect whereof the transaction is concluded (money, real estate and similar), and the value thereof (amount of money and currency in which the Monetary operation or transaction is performed, the market value of the Property and similar);

(C) information about the person – the beneficiary of the funds (for a natural person – given name and last name, date of birth, personal identification number, or another unique sequence of symbols assigned to that person intended for the identification of the person, citizenship; for a legal person – name, legal form, registered office address, and code (if any has been assigned), except when fund transfers are made in accordance with Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006. In such case, information provided therein is recorded on the beneficiary of the funds.

In addition to the information specified above, the log of suspicious operations and transactions shall also contain information about the Beneficial owner (given name and last name, date of birth, personal identification number or another unique sequence of symbols assigned to the person for identification purposes, citizenship) and indicate which suspicious operation or transactions criterion specified in this manual a particular case meets.

The log of Customers with whom transactions or Business relationship have been terminated must contain the information specified above, as well as information about the Beneficial owner (first and last name, date of birth, personal identification number or another unique sequence of symbols assigned to the person for identification purposes, citizenship) and motives for termination of transactions or Business relationship.

Information must not be entered into the log specified in Item (B) where the Customer is another financial institution or a financial institution of another European Union Member State.

The logs can be stored and managed electronically.

Data shall be entered in the logs in chronological order, on the basis of the documents supporting the Monetary operation or transaction or other instruments with legal effect related to performance of the Monetary operations or conclusion of transactions, immediately however within three business days as of the date of performance of the Monetary operation or conclusion of transaction.

Data shall be entered in the log of Customers with whom transactions or Business relationship have been terminated in chronological order within three business days as of the date when the specified circumstances occurred or were established.

Transactive must collect and, upon the FCIS's requirement, provide the following data about the Beneficial owner: identification data of the Beneficial owner, evidence of verifying the information provided by the Customer using reliable and independent sources, information about the management structure of the Customer (legal entity).

7.2 The Customer File

During business, Transactive creates Customer Files for all Customers with whom it has an ongoing service agreement. The Customer File consists of:

- the Merchant Application Form which is a Customer information record setting out the Customer's name, address and the nature of their principal business, and their service and operational requirements;
- the ongoing service agreement or contract;
- all documents used for identification of the Customer including corporate documents and individual identification documents;
- a record of the purpose and intended nature of the Business relationship;
- records about the persons who sign the agreement on behalf of the entity, the employees authorised to order transactions under the agreement and records of the directors, the Beneficial owners of the entity, records about third parties, including names, addresses, dates of birth and occupations, as applicable;
- internal memoranda and correspondence, which includes any memo, note, email, message or similar communication that is created or received, in the normal course of business, about the services provided to the Customer.

7.3 Customer Data Maintenance

Significant changes in the details and information on a Customer will be obtained from an authorised person, such as a director or authorised signatory.

Significant changes include (but are not limited to):

- change of name;
- change of address;
- change of banking/wiring instructions;
- change of owners, directors, authorised persons and contacts.

These changes cannot be made via phone. The document of record will be held in the Customer File on the same retention terms as other records.

7.4 Other Records to be Kept

7.4.1 Politically Exposed Person Records

Once a PEP transaction has been reviewed by senior management a record will be kept of:

- the office or position of the individual who is a Politically exposed person;
- the source of the funds (wealth and income), if known, that were used for the transaction;
- the date it was determined the individual to be a Politically exposed person;
- the name of the member of senior management who reviewed the transaction; and
- the date the transaction was reviewed.

7.4.2 Customer Due Diligence and other Records

Data of the registration logs specified shall be stored in paper or in electronic form for a period of **eight years** as of the closing date of transactions or the end of Business relationship with the Customer.

Copies of documents verifying the Customer's identity, identification data of the Beneficial owner, live video transmission (live video broadcast) record, other data received during identification of the Customer, documents related to accounts and/or agreements (original documents or documents in an electronic form, saved in accordance with the Description on the Procedure for Selecting and Saving Paper Documents in Electronic Form) shall be stored for a period of **eight years** as of the closing date of transactions or the end of Business relationship with the Customer.

Correspondence related to the Business relationship with the Customer shall be stored in paper or in electronic form for a period of **five years** as of the closing date of transactions or the end of Business relationship with the Customer.

Documents confirming the Monetary operation or transaction and data or other instruments with legal effect, and data related to performance of the Monetary operations or conclusion of the transactions shall be stored for a period of **eight years** as of the date of performance of the Monetary operation or conclusion of the transaction.

Letters by which findings of the investigation on operations that, by virtue of their nature, may be related to Money laundering and Terrorist financing, and complicated and unusually large transactions in particular, as well as any unusual transaction structure that does not have an evident economic or visible legal goal, and Business relationship or Monetary operations with Customers from third countries that, pursuant to official information from inter-governmental organisations, do not enforce adequate Money laundering and Terrorist financing prevention measures or enforce measures that are not aligned with the international standards. The results of investigation of the grounds and purpose of such Monetary operations shall be documented in writing and stored in paper or electronic form for a period of **five years**.

The time limits for record keeping may be extended additionally for no longer than two years upon a reasoned instruction of a competent authority.

Transactive must ensure that the documents and information were stored irrespective of whether: (a) the Monetary operations or transactions are local or international; (b) Business relationship with the Customer continues or have ended.

Transactive must ensure the documents were stored so that it would be possible to retrieve specific Monetary operations or transactions and upon necessity, to provide them and information set out therein to the FCIS or other competent authorities.

7.4.4 CCO Reports

All CCO reports to senior management will be kept indefinitely.

7.4.5 Training Records

The firm maintains records of all AML training undertaken by staff, the date it was provided and the results of any tests if applicable. These records will be kept for 5 (five) years following the end of employment with the firm.

7.4.6 Suspicious or Unusual Monetary Operation or Transaction Report Records

All SUTs submitted including correspondence with the FCIS, the Bank of Lithuania (or any other government agency) will be kept for the time required under applicable laws.

Internal reports of suspicions will be kept for 10 (ten) years.

7.5 General Exceptions to Record Keeping

If information in a record is already readily available in any other record then we do not have to keep that information again.

7.6 How Should Records Be Kept?

All confidential documents are kept in electronic format even if received initially in paper format. Documents received in paper format are only kept if they are original documents, and are kept in a locked fire proof safe. Once scanned they are not referred to or consulted on a regular basis.

Confidential documents are kept electronically on cloud servers using Dropbox Business. This service is protected via access controls to ensure that data is not improperly disclosed, modified, deleted or

rendered unavailable. Logs track all access to such data and identify who and when the data was accessed. Documents which are deleted are held on the server for 180 days. Confidential documents with personal (Customer) information are held in accordance with regulatory requirements even after the Customer relationship has ended.

Employees who have been authorized to view information at a particular classification level will only be permitted to access information at that level or at a lower level on a need to know basis.

All access to systems are configured to deny all but what a particular user needs to access per their business role.

Access to systems or applications handling confidential information follows the data access request process. All requests require approval by the Chief Technology Officer (CTO). Access to data exceeding the employee's authorized role must also follow the data access request process and includes documented limits around such access (e.g. access source, access time limits, etc.).

If a new or existing user requires access to confidential data, a HelpScout support ticket is opened and the access is implemented after approval by the CTO.

Each user's access privileges shall be authorized according to business needs. All privileges must be assigned based on job classification and function.

The use of non-authenticated (e.g. no password) user IDs or user IDs not associated with a single identified user are prohibited. Shared or group user IDs are never permitted for user-level access.

Every user will be assigned a unique user ID and a personal secret password for accessing Transactive's files and records.

7.7 How Long Must Records Be Kept?

Unless otherwise explicitly specified in the applicable laws all records will be kept for a minimum of eight years after the transaction or when they were created, or in the case of Customer information records, until eight years after the account has closed.

These records include applications that were declined, and cancelled applications unless the application was cancelled before it was considered by the account approval process.

8 Ongoing Monitoring and Enhanced Due Diligence

Transactive will implement a risk-based approach to identify potential high risks of Money laundering and Terrorist financing and develop strategies to mitigate them.

8.1 The Risk-Based Approach

In Money laundering and Terrorist financing, a risk-based approach covers the following:

- the risk assessment of Customer relationships and business activities;
- the risk mitigation to implement controls to handle identified risks;
- keeping Customer identification, beneficial ownership and Business relationship information up to date; and
- the ongoing monitoring of Business relationships and transactions.

Existing regulatory obligations, such as for Customer identification, are a minimum baseline requirement. Where enhanced due diligence is appropriate, a principle of the risk-based approach is to focus resources where they are most needed to manage risks within our tolerance level.

8.2 Risk Mitigation

Risk mitigation is implementing controls to limit the potential Money laundering and Terrorist financing risks identified in the risk assessment so as to stay within the risk tolerance level. When the risk assessment determines that risk is high for Money laundering or Terrorist financing, then we will develop risk mitigation strategies and apply them.

In all situations, risk mitigation controls and measures include:

- focusing on operations (products and services, Customers and Business relationships, geographic locations, and any other relevant factors) that are more vulnerable to abuse by money launderers and criminals;
- informing senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious transaction reports filed;
- providing for program continuity despite changes in management, employees or structure;
- focusing on meeting all regulatory record keeping and reporting requirements, recommendations for anti-Money laundering and anti-Terrorist financing compliance and providing for timely updates in response to changes in requirements;
- enabling the timely identification of reportable transactions and ensure accurate filing of required reports;
- incorporating anti-Money laundering and anti-Terrorist financing compliance into job descriptions and performance evaluations of appropriate personnel; and
- providing for adequate supervision and training of employees that handle currency transactions, complete reports, monitor for suspicious transactions, or engage in any other activity that forms part of the anti-Money laundering and anti-Terrorist financing program.
- increasing awareness of high risk situations within all business lines;
- increasing the frequency of ongoing monitoring of transactions or Business relationships;
- escalating the approval of the establishment of an account or relationship even if not otherwise required to do so;
- increasing the levels of ongoing controls and reviews of relationships;
- requesting high-risk Customers to provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers and terrorists;
- verifying the identity of Customers by reference to reliable, independent source documents, data or information;

- preventing any transaction with a potential Customer until identification and account opening information has been obtained;
- implementing an appropriate process to approve all relationships identified as high-risk as part of the Customer acceptance process or declining to do business with potential Customers because they exceed Transactive's risk tolerance level;
- implementing a process to exit from an existing high-risk relationship which management sees as exceeding Transactive's risk tolerance level.

8.3 Ongoing Monitoring Obligations:

Ongoing monitoring means monitoring Customer relationships on a periodic basis, keeping a record of the measures taken to monitor the relationship and the information obtained, keeping a record of the purpose and intended nature of the business relationship and reviewing and updating this information periodically.

The risk assessment of the Customer determines how frequently we will monitor each Business relationship and how frequently that Business relationship information is to be kept up to date. Frequency of Customers' risk re-assessment is described in a separate procedure.

Ongoing monitoring of each Business relationship is intended to:

- detect suspicious activity that must be reported;
- keep Customer identification, the purpose and intended nature of the Business relationship, and beneficial ownership information up to date;
- reassess the level of risk associated with the Customer's transactions and activities;
- determine whether the transactions or activities are consistent with the information previously obtained about the Customer, including the risk assessment;
- understand a Customer's activities over time so that any changes can be measured to detect high risk.

These requirements do not need to follow the same timeframe, so long as high-risk Customers are monitored more frequently and with more scrutiny than low-risk Customers. Monitoring high-risk situations may include measures such as:

- reviewing transactions based on an approved schedule that involves management sign-off;
- developing reports or performing more frequent review of reports that list high-risk transactions, flagging activities or changes in activities from expectations and elevating concerns as necessary;
- setting business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
- reviewing transactions more frequently against suspicious transaction indicators relevant to the relationship.

Where ongoing monitoring finds that a Business relationship is high risk, then the risk assessment will treat that Customer as high risk. This means more frequent monitoring of the Business relationship with that Customer, updating their Customer identification information more frequently, and adopting any other appropriate enhanced monitoring measures (as listed below).

The frequency of monitoring will vary depending on the risk assessment of the Customer but the ongoing monitoring obligation is to monitor all Business relationships.

The current scheduled frequency of review (monitoring the Business relationship and updating Customer identification information) is that high-risk Customers will be reviewed annually, moderate risk Customers will be reviewed within two years and low-risk Customers will be reviewed within three years.

8.4 Enhanced Due Diligence

Where the risks of Money laundering or Terrorist financing are higher, the Customer will be classified as high risk and we will conduct EDD measures, consistent with the risks identified.

For EDD reviews, the compliance team will complete a standard form which lists all the measures that will be taken. Here is a non-exhaustive list of enhanced measures that will be taken to mitigate the risk in cases of high-risk Business relationships :

- obtaining additional information on the Customer (e.g. occupation, volume of assets, information available through public databases, Internet, etc.);
- updating more frequently the identification of the Customer and any Beneficial owner;
- obtaining information on the source of funds or source of wealth of the Customer;
- obtaining information on the reasons for intended or conducted transactions;
- obtaining the approval of senior management to enter into or maintain the Business relationship;
- identifying patterns of transactions that need further examination;
- requiring the first payment to be carried out through an account in the Customer's name with a European Union regulated credit institution or one from an equivalent jurisdiction;
- increased and more frequent monitoring of transactions particularly of higher-risk products, services and channels;
- establishing more stringent thresholds for ascertaining identification;
- gathering additional documents, data or information; or taking additional steps to verify the documents obtained;
- establishing transaction limits customised to the nature, scale and complexity of the Customer;
- increasing internal controls of high-risk Business relationships;
- obtaining the approval of senior management at the transaction level for products and services that are new for that Customer;
- obtaining additional information on the intended nature of the Business relationship;
- obtaining regular credit reports;
- undertaking a site visit;
- structured online research of entities, including reviews of industry data, and the use of and documentation of results of an adverse keyword search string;
- summaries of account activity.

EDD measures described in Section 6.4 herein will be applied at all times.

8.5 Termination of Business Relationships

Essential to an effective AML / CTF Policy is the requirement to terminate Customers in order to prevent the risk of financial crime and to protect the reputation of the firm.

Transactive will terminate and demarket any Customers or Business relationships where the risks are too high as well as where there is no business case for continuing the relationship. Terminating a Customer is considered the last step in the risk mitigation process and the decision is taken seriously. Prior to termination many other review and analysis steps are taken. Termination is not necessarily dependent on one factor only, but is rather an accumulation of many factors, however if the Customer avoids or refuses to submit, and following a request from Transactive, information about the origin of funds or Property, other additional data, Transactive may takes steps to terminate the transactions or Business relationship with the Customer.

9 Suspicious or Unusual Monetary Operations or Transactions

Any Suspicious monetary operations or transaction (SUT) must be reported to the FCIS. This will be done by the CCO or in their absence by their designated nominee or deputy.

When a SUT is detected that operation or transaction must be suspended and a report made to the FCIS within three hours. There is no minimal threshold or limit for such a report. Once a SUT is reported to the FCIS then they are required to respond within ten working days. If the FCIS requests further information then that request has to be responded to immediately.

If a SUT Report is made in good faith to the FCIS and the transaction or operation is delayed for ten working days there is no liability against the firm from the Customer.

Any member of Transactive will report SUTs to the CCO. A suspicious activity is one where it is known, or suspected, there are reasonably grounds to know or suspect that a person is engaged in, or attempting, Money laundering or Terrorist financing.

9.1 Grounds for Knowledge or Suspicion

Having knowledge means knowing something to be true. Knowledge can be inferred from the surrounding circumstances; so, for example, a failure to ask obvious questions may imply knowledge. The knowledge must, however, have come to Transactive during the course of business, or from a disclosure (to the CCO).

Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion is more than speculation and is based on some foundation.

The results of investigation of the basis for and purpose of performance of such operations or transactions must be substantiated by documents and must be stored for ten years.

Members of staff who consider a transaction or activity to be suspicious, would not necessarily be expected to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or Property were those arising from a crime or Terrorist financing. “Reasonable grounds to know or suspect” introduces an objective test of suspicion. The test is likely to be met when there are facts or

circumstances, known to the member of staff, from which a reasonable person (in a payments firm) would have inferred knowledge, or formed the suspicion, that another person was engaged in Money laundering or Terrorist financing.

A defence of failing to meet the test of suspicion, would be for staff to demonstrate that they took reasonable steps to know the Customer and the rationale for the transaction, activity or instruction.

9.2 How to Make a Suspicious Transaction Report

Any member of staff, who is suspicious that a transaction may involve Money laundering or who becomes aware during the course of their work that someone else is involved in Money laundering, must make a disclosure to the CCO using an internal SUT report form.

Once completed, the form should be printed off. The member of staff making the report must sign and date the form and send to the CCO.

The form must then be hand delivered by the reporting member of staff to the CCO. The CCO will sign a receipt to show date and time of report.

Upon receipt of the form by the CCO, they will then decide what is to be done as a result of the report, e.g., whether the matter must be reported to the FCIS or not, or further enquiries made and record its decision and the reason for it in the Customer files. The member of staff concerned must be informed of the decision and the reasons for it.

If the matter is referred to the FCIS the CCO will be responsible for completing the FCIS report form and discussing with the reporting member of staff how matters with the Customer are to be conducted from that stage, bearing in mind that the law prohibits us from continuing with the 'prohibited act' which is being reported to FCIS. The FCIS report form must be signed off by the CCO or the managing director.

In accordance with the tipping off provisions of the law and regulations, the report must not be discussed with the Customer.

We cannot proceed with a transaction whilst we await consent from the FCIS (who have ten working days to consider the report).

The CCO will report using one of the existing standard.

Any paper file for each matter will be kept by the CCO.

There must be no record on the Customer File or on the computer system which refers in any way to suspicious activity reporting, Money laundering, etc., to avoid the risk of tipping off. It is forbidden by law to inform a Customer that a SUT Report has been submitted, or to inform them of an investigation into their affairs.

All records of SUT Reports will be kept in the central reporting file, which is kept by the CCO.

9.3 How to Identify a Suspicious or Unusual Monetary Operation or Transaction

Monetary operations and transactions may give reasonable grounds to suspect that they are related to Money laundering or terrorist activity financing regardless of the sum of money involved. There is no monetary threshold for making a SUT Report. Suspicious transactions may involve several factors that on their own seem insignificant, but together raise suspicion that the transaction is related to the commission or attempted commission of a Money laundering or terrorist activity financing offence, or both. As a general guide, a transaction may be connected to Money laundering or Terrorist financing activity financing when we think that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust.

Transactive will examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose.

The context in which the transaction occurs or is attempted is a significant factor in assessing suspicion and this will vary from business to business and from one Customer to another.

Transactions will be evaluated in terms of what seems appropriate and is within normal practices in business, and based on our knowledge of the Customer. The fact that transactions do not appear to be in keeping with normal industry practices may be a relevant factor.

Reasonable evaluation of relevant factors, including the knowledge of the Customer's business, financial history, background and behaviour is the basis of assessing suspicion. Behaviour is suspicious, not people. We have listed below some indicators to help with this assessment.

9.4 Indicators of Suspicious or Unusual Transactions

Certain products, services, activities or channels may pose a higher risk of misuse for Money laundering. Listed below are several anti-Money laundering risk indicators or “red flags” that might be grounds for suspicion. The list is not exhaustive and not conclusive, but will be used as a guide for inquiry and follow-up, alongside other material.

A single indicator does not necessarily indicate reasonable grounds to suspect Money laundering or Terrorist financing activity. However, if several indicators are present during one or a series of transactions, then we will take a closer look at other factors before deciding whether the transaction must be reported.

In the case of a transaction aborted in the belief that the Property is owned or controlled by or on behalf of a terrorist or a terrorist group, then there must be a terrorist property report. If there are reasonable grounds to suspect that the transaction is related to an attempted commission of a terrorist activity financing or Money laundering offence, then a suspicious transaction report about the attempted transaction is also required.

Becoming aware of certain indicators could trigger reasonable grounds to suspect that one or more transactions from the past (that had not previously seemed suspicious) were related to Money laundering or Terrorist financing.

9.4.1 Criteria of Suspicious or Unusual Transactions

An non-exhaustive list ofcriteria for recognizing Money laundering and Suspicious monetary operations or transactions related to the behaviour of the Customer is as follows:

(A) at the time of entering into a Business relationship, the Customer or their representative is reluctant to provide information necessary to identify the Customer, conceals the identity of the Beneficial owner or avoids providing the information necessary to identify Beneficial owners, provides documents which raise doubts as to their genuineness, authenticity etc.;

(B) it is difficult to obtain information or documents necessary for the monitoring of the Business relationship from the Customer: it is difficult to contact the Customer, their place of residence as well as other contact details often change; the phone number provided by the Customer or his representative does not answer or it is disconnected; the Customer or their representative fail to respond when addressed via e-mail;

(C) the Customer is unable to answer questions regarding their ongoing/planned financial activity and the nature thereof; is excessively nervous;

(D) the Customer expresses a wish to end the Business relationship when asked to provide the information necessary for monitoring of their Business relationship;

(E) at the request of Transactive, the Customer refuses to provide information on the origin of the funds deposited (or an attempted deposit) to their account and/or to support it by relevant documents;

(F) a single individual is a director or the Beneficial owner of multiple legal entities (except for big groups of companies);

(G) several companies have been registered at the same address as the one of the Customers or their representative.

The criteria for recognizing Money laundering and Suspicious monetary operations or transactions related Monetary operations or transactions carried out by the Customer or his representative are as follows:

(A) the Monetary operations or transactions of the Customer are not in line with the activities indicated in their incorporation documents or not in line with what was discussed at on-boarding with Transactive;

(B) the nature of the Monetary operations or transactions conducted by the Customer raise a suspicion of efforts to avoid various identification or verification steps set forth by Transactive;

(C) the Customer's account is a pass-through account: having credited the funds to the account, they are transferred to another account shortly afterwards, and other operations barely take place on the account;

(D) during the enhanced review of the Customer's source of funds - the flow of goods and settlements made for them do not match: companies or individuals unrelated to the transaction appear to pay for the goods;

(E) the Customer carries out a transaction (transactions) and make a payment (payments) which is (are) beyond the Customer's possibilities known to Transactive or requests to make an advance payment exceeding the regular amount or other type of payment;

(F) the Customer requests that funds belonging to them are paid to persons who are clearly unrelated to the Customer's normal activity;

(G) the whole payment or part of a payment is made on the Customer's behalf by persons who are clearly unrelated to the Customer or their normal activity;

(H) the Customer is continuously engaged in transactions for Property where the value is clearly not in line with the average market value;

(I) the Customer carries out Monetary operations or conducts transactions without any apparent economic justification;

(J) the Customer carries out Monetary operations or conducts transactions when it is difficult or impossible to identify the Beneficial owner;

(K) the Customer, the Customer's representative (where the Monetary operation or transaction is carried out through the representative) or the person who is the beneficiary of the Monetary operation or transaction is subject to financial sanctions in the framework of the Law on the Implementation of Economic Sanctions of the Republic of Lithuania and other International Sanctions;

(L) the number of transfers from different accounts to the Customer's account increases without a clear basis;

(M) the number of transfers from the Customer's account to several different unrelated accounts increases without a clear basis;

(N) Non-Profit Organisation's ("NPO") monetary operations or transactions are not in line with the types of activity specified in its incorporation documents;

i. only crediting or cashing operations are performed in the NPO's account;

ii. purpose of a payment order to/from the NPO does not match the activity conducted by a beneficiary or a donor;

iii. large payment orders are made to the accounts of founders of the NPO;

iv. the NPO's account is replenished by small amounts more often without an apparent basis.

The criteria for recognising Money laundering and Suspicious monetary operations or transactions related to the geographical aspect of the Monetary operations or transactions carried out are as follows:

(A) the Customer does not perform monetary transfers from/to its account opened in a European Union Member State, in which it has been registered, or the amount of funds transferred to the Customer's account opened in the state of registration thereof constitutes a negligible part of all the Monetary operations over time or the funds kept in it;

(B) Monetary operations or transactions are carried out with natural and legal persons located in high-risk regions (e.g. Sanctioned countries; countries which are not members of the FATF or countries that have been highlighted by FATF as uncooperative; or with countries where terrorist organizations are very active) whereas the economic justification of the Monetary operations or transactions is unclear;

(C) the Customer constantly performs Monetary operations or conducts transactions with legal entities or other organisations, registered in the target Areas, as defined in the Law on the Corporate Income Tax of the Republic of Lithuania, when there is no clear economic justification of such activity;

(D) there is data suggesting that a person donating funds to the NPO may be fictitious or represent a person originated from a risk country and/or the donated funds do not match the person's financial status;

(a) a NPO, operating in a risk country, or a person who provides support to risk countries carries out payment orders or makes money remittances to a person located in Lithuania;

(b) a donation to a NPO is accompanied by a condition to transfer funds to a person associated with a risk country.

Seeking to recognize the likely features of Terrorist financing, the following criteria shall be taken into consideration:

(A) place of birth, place of residence, citizenship or nationality of a Customer or Customer representative is associated with the risk country and/or the natural person is associated with a legal entity registered in the risk country;

(B) Monetary operations are carried out by legal entities established in a risk country or target area, or established legal entities which carry out Monetary operations through other legal entities established in those areas or countries;

(C) there is information leading to assumption that a Customer does not act for his own benefit and/or may represent a person associated with a risk country or target area, or a person is reluctant to reveal the true Beneficial owners;

(D) a Customer is unable to explain why they require Transactive services, what kind of activity they intend to conduct or are unable to provide other necessary information;

(E) a Customer requests that correspondence related to the financial operations are sent to an address located in a risk country;

(F) a Customer receives or makes payment orders, transfers to/from the account of a person who is associated with a risk country or registered in the target area;

(G) during the enhanced review of the Customer's source of funds a one-time replenishment of the Customer's bank account by an unusually large amount is identified, which is extraordinary to the Customer's activity and is cashed out or otherwise transferred immediately;

(H) access to the Customer account is granted to several authorized persons unrelated to the Customer by family or partnership relations and/or if those persons are associated with a risk country;

(I) payment orders for services provided by a Customer registered in a risk country or target area which are not related with their activity, and/or withdrawing funds shortly after the payment order;

(J) the purpose specified in the payment order to a risk country is for example, as follows: *dole, donation, sadaqa, sadaga, zakat, zakaat, ramadaan, ei al'adha, iftar, haj, sponsor aid*;

(K) during a transaction, at least one of the parties thereto is reluctant to provide information necessary for identification of the Customer;

(L) a transaction is settled in a currency of a risk country;

(M) a Customer, associated with a risk country or target area, makes a payment order for real estate;

(N) a Customer, associated with a risk country or target area, intends to receive assistance from persons providing legal services in order to settle a transaction seeking to conceal the origin of the funds.

In assessment of the alleged connection of the Property with the Terrorist financing, the following aspects must be taken into consideration:

(A) funds shall mean any type of tangible or intangible, movable or immovable Property irrespective of the way of acquisition thereof and legal documents or instruments of any form, including electronic or digital, evidencing title to or an interest in such Property, including, however not limited to, bank credits, traveller's cheques, bank cheques, postal money orders, shares, securities, bonds, notes, letters of credit;

(B) the Property (funds) may be of either legal or illegal origin, as long as it is collected, accumulated or provided for purposes of the Terrorist financing;

(C) both direct and indirect collection, accumulation or provision of the Property (funds) shall be treated as the Terrorist financing activity;

(D) collection, accumulation or provision of the Property (funds) shall be regarded as intentional deliberate activity seeking or knowing that this Property (funds) or only a part thereof will be aimed at the Terrorist financing, i.e. mere perception of a person that the Property might be aimed at the Terrorist financing is sufficient, even if he does not have an intentional pursuit thereof;

(E) Terrorist financing includes collection, accumulation, provision of the property (funds) for committing particular terrorist crimes (e.g. to perform a terrorist attack), training of terrorists (e.g. inciting crimes of terrorism, recruiting, training terrorists, creating terrorist groups etc.), and also supporting individual or several terrorists or terrorist groups even if this Property will not be aimed at committing particular terrorist crimes (e.g. for the rent or premises, material support, healthcare, relief etc.). It shall not be necessary to establish a connection of the collected, accumulated, provided Property (funds) with a particular terrorist crime.

9 Final Provisions

The AML / CTF framework implemented in the firm shall be reviewed (and updated, if necessary) at least once a year, or, as required, e.g. after new legislation has been adopted, change in the business profile of the firm and risks inherent thereto occurs, taking into consideration results of internal or external AML audit, etc.

The Policy shall be amended and/or supplemented by the decision of the Board of Transactive.

The CCO shall be responsible for familiarising employees of Transactive with the Policy. The employees will be familiarised with the Policy upon signature. Employees who violate the requirements of the Policy will be held liable in accordance with the procedure established by law.

Appendix 1 – Glossary of Abbreviations

Abbreviations used in this document:

AML	Anti-Money laundering
CTF	Combating terrorist financing
EEA	European Economic Area
EU	European Union
FATF	Financial Action Task Force, an intergovernmental body whose purpose is to develop and promote broad AML/CTF standards, both at national and international levels
FCIS	Financial Crime Investigation Service, the financial intelligence unit in Lithuania
PEP	Politically Exposed (natural) Person
SUT	Suspicious Monetary Operation or Transaction