STREAMFLOW EOOD

Fraud Management and KYC

Policy and Procedures

Annual Policy Review

This Policy Statement was last reviewed on the 26th June 2020. Any questions about this policy or suggestions for additions that staff would like to be considered on review should be directed to the MLRO. After any annual risk assessment, the AML policy shall be reviewed.

Version Control

Version	Date	Amendment comments	By whom	Approved by
1.2	24.05.19	Policy revision		
1.3	26.06.20	Revised to include PEPs/Sanctions, Prohibited Countries/Industries List and Record Keeping	AML dept	

Table of Contents:

1. INTRODUCTION

STREAMFLOW EOOD has a legal, moral and social responsibility to its customers to deter and detect those who would seek to use STREAMFLOW EOOD to facilitate the movement of criminal funds, and funds designed to finance terrorism.

The objectives of this Policy are to:

- Provide a consistent approach across the STREAMFLOW EOOD to the deterrence and detection of those suspected of laundering the proceeds of crime or those involved in the funding or execution of terrorism, and the disclosure to the relevant authorities.
- Explain clearly the responsibility of the Senior Management team, the Money Laundering Reporting Officer (MLRO) and other key colleagues.
- Set out requirements for effective implementation and monitoring of compliance with this policy.

This Policy applies to all colleagues working within STREAMFLOW EOOD and includes agency workers, self-employed or contract workers and any individual on work experience (including interns).

1.1 Money Laundering – what is it?

Money laundering comprises, in summary, being in possession of, or dealing in any way, or assisting another party in connection with, property arising from any criminal offence, including terrorist related activities. Accordingly, if suspicion is formed about such an activity, it needs to be reported to the Money Laundering Reporting Officer (MLRO) for consideration, which in this case is the External Consultant. Criminal property means any pecuniary or proprietary benefit arising from criminal conduct.

Money laundering also includes any matters connected with funds being used or provided for any terrorism related purpose where no other crime may have taken place. We are not required to become experts in criminal law. But we should apply our general knowledge and experience in seeking to fulfil our legal obligations.

Apart from the more obvious offences relating to drugs trafficking, terrorism, fraud, theft and false accounting, and such offences as you may be aware of from service line specific knowledge, consideration also needs to be given to other potential offences which may well be encountered in business. These include bribery, corruption and criminal breach of competition. If in doubt, we should contact our advisor, which plays the relevant role in such cases.

1.2 Fraud – what is it?

Fraud, for the purposes of these procedures, relates to actions taken by potential or existed customers to make fraudulent moves and transactions to the detriment of our company by using false identities and personal details &/or false credit card details to deposit and withdraw money which will possibly be reclaimed at a later stage through a chargeback by the rightful owners.
Fraud could also relate to a legitimate customer who falsely claims that his credentials-ways of payment (e.g. Credit Card) was used without his knowledge so that he can recover monies lost on bets. Internal fraud is covered by other internal controls and procedures implemented by STREAMFLOW EOOD.

2. GENERAL POLICY KYC-AML

2.1 STREAMFLOW EOOD shall only carry on business with persons whom they have adequately identified and in whom there is no suspicion of criminal or terrorist activity.

2.2 STREAMFLOW EOOD shall not accept to open anonymous accounts or accounts in fictitious names such that the true beneficial owner is not known.

2.3 STREAMFLOW EOOD shall not accept customer residing from a non reputable jurisdictions.

2.4 STREAMFLOW EOOD shall keep at all times a secure online list of all registered customers and also keep contact with them.

2.5 STREAMFLOW EOOD must not launder money or assist others to do so intentionally or otherwise.

2.6 STREAMFLOW EOOD shall take all measures necessary to detect and prevent fraudulent customers and activity through regular monitoring.

2.7 STREAMFLOW EOOD must not impede, by action or inaction, any official investigation of money laundering.

2.8 STREAMFLOW EOOD personnel must report any suspicion of money laundering to the MLRO – The External Auditor- Counsellor.

2.9 The personnel shall affect all Anti-Money Laundering Actions through its MLRO who will in turn escalate the reports as necessary.

2.10 STREAMFLOW EOOD shall, as much as possible, follow the relevant 40 + 9 recommendations of the Financial Actions Task Force (www.fatf-gafi.org).

2.11 STREAMFLOW EOOD shall follow all the laws and regulations relating to anti-money laundering and prevention of terrorism.

2.12 STREAMFLOW EOOD shall provide the necessary training for its personnel in anti-money laundering and fraud procedures.

2.13 STREAMFLOW EOOD shall keep records of all procedures carried out and reporting effected.

3

3. MANDATORY REQUIREMENTS

3.1. Organisation

Adequate and competent resource must be in place to manage ML/TF risks effectively and must be organised to minimise the risk of facilitating the movement of suspected criminal property whilst complying with legal and regulatory requirements.

3.2. Money Laundering Reporting Officer

To meet regulatory requirements, all STREAMFLOW EOOD is required to appoint a Money Laundering Reporting Officer. Mr Vissarion Karvounis is the appointed Money Laundering Reporting Officer (MLRO). He can be contacted on the following phone / fax numbers:

Phone number: +359 32 940 003
Fax number: +359 32 940 003
Mobile: +359 87 644 5944
Email: vk@streamflow.bg

3.3. Responsibilities

Senior Management are responsible for:

- The establishment and management of effective systems and controls to counter the risks of Money Laundering and Terrorist Financing.
- The day to day compliance with money laundering obligations within the areas of the STREAMFLOW EOOD for which they are responsible.
- Ensuring that the MLRO is provided with prompt advice of unusual/suspicious transactions and other matters of significance.
- Seeking from the MLRO, at least annually, a report relating to the STREAMFLOW's compliance with its anti-money laundering obligations and acting on the findings and recommendations.

The STREAMFLOW's MLRO is responsible for:

- Undertaking the Senior Manager Function role (SMF) for the STREAMFLOW.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations.
- Developing internal procedures. MLRO will ensure that this internal policy is kept up to date with new ML/TF requirements and developments.
- Ensuring that staff are aware of their obligations and the STREAMFLOW's procedures, that staff are adequately trained in money laundering prevention, their legal and regulatory responsibilities and their role in handling criminal property and money laundering/terrorist financing and risk management.
- Carry out regular assessments of the adequacy of the STREAMFLOW EOOD 's systems and controls to ensure that money laundering risks are managed effectively.
- Representing the STREAMFLOW EOOD to all external agencies in the Bulgaria, and in any other third-party enquiries in relation to money laundering prevention or compliance.
- Co-ordinating Senior Management focus on managing money laundering/ terrorist financing risk and ensuring that all parts of the STREAMFLOW EOOD are complying with the stated policy and therefore monitoring operations and development of the policy to this end.
- Preparing regular compliance reports to the Board and Senior Management.
- Ensuring that all employees complete the Half-Yearly Suspicious Transaction Reports.
- Receiving and reviewing internal disclosures and determining as to whether a report needs to be disclosed to the State Agency for National Security.

- Obtaining and making use of national and international findings concerning countries with serious deficiencies.
- Submit an Annual Risk Report to the State Agency for National Security annually.
- Undertake an annual review of sanction screening and suspicious activity monitoring systems to check effectiveness.
- Ensure that there is appropriate transaction monitoring in place to monitor Correspondent Partners.

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering/ terrorist financing.
- Complying fully with all money laundering/ terrorist financing procedures in respect of customer identification, account monitoring, record keeping, reporting, and training and competence requirements.
- Reporting all suspicions of money laundering to the MLRO.
- Promptly completing, every 6 months, the Suspicious Transaction Acknowledgement Form confirming that they had no suspicions during the previous six months or that any suspicions have been reported.

Internal Audit is responsible for:

- Auditing compliance by the STREAMFLOW EOOD with money laundering statutory and regulatory obligations, in respect of the STREAMFLOW EOOD ’s money laundering policy and procedures.
- Advising Senior Management of any deviations from the STREAMFLOW EOOD ’s policies and procedures that have been noted by Internal Audit during their reviews.

4. KYC PROCEDURE

4.1. STREAMFLOW EOOD' approach

- We should only do business with customers whom we believe to be of good character, integrity and reputation, and whose wealth and funds are only derived from legitimate sources. Therefore we are going through analytical Know Your Customer (KYC) Procedures.

- We should endeavour to establish the identity of our customers as soon as is reasonably and practically possible where deposit turnover exceeds €2.000 per day or over €15,000 per month whichever happens first. This only goes, with our registered customers in our data-base.

- We are inter-mediators of cash handling- via electronic vouchers or similar means of handling and transferring money, ***only***, with well-respected Credit, E-Money institutions as well as Publicly Known Institutions or Regulated Banking Institutions. Our Major Clients- are considered to be these Institutions.

- We do not Co-operate or have any business relationship with shell banks- and we do not intent to.

- We wish to do business only with well-respected rated Institutions, and therefore we ask them to provide us with their

    - Publicly known Ranking

    - KYC and AMC Policies and Procedures

- Permissions or chart of authorities, for conducting relevant business in their based country.

- We should obtain reasonable information, adequately documented and corroborated, about the identity of all our customers when required to do so, if there is doubt about the authenticity of the customer or when money transferring figures raise concern.

- From the information gathered, we should be able to obtain a ***reasonable assurance*** about the identity of our customer and that he or she is not involved in any criminal or terrorist activity or activities.

- If we should develop suspicions of money laundering activities regarding a client or a proposed client, or any third party observed in the course of our business, (wherever that client or third party may be located) we should report promptly to the company's Money Laundering Reporting Officer (MLRO). The MLRO will investigate, analyze, consult and, if appropriate, report the activity to authorities and also BNB. The company reserves the right to take any other action considered legal and necessary.

4.2. Anti - Money Laundering and Fraud Guidance- Terminology

This Guidance is based on Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, the Bulgarian Anti Money Laundering Act (2018) and the regulatory requirements and FATF40+9 recommendations – breach of which may well result in legal liability for the company and/or the individuals concerned. Adherence to this Guidance is, therefore, important for your protection as well as that of the company.

Legalization of Revenue that may come from criminal activities (ML- MONEY LAUNDERING), **money laundering within the meaning of the Art. 2 of the Bulgarian AML Act when committed intentionally is:**

1. the transformation or transfer of property, knowing that such property has been acquired from a criminal activity or from an act of participation in such activity in order to conceal or conceal the unlawful origin of the property or to assist a person involved in such an act in order to avoid the legal consequences of that person's conduct;
2. the concealment or concealment of the nature, source, location, movement, rights in respect of, or ownership of property, knowing that such property has been acquired by a criminal activity or by an act of participation in such an activity;
3. the acquisition, possession, holding or use of property knowing at the time of receipt that it has been acquired by a criminal activity or an act of participation in such an activity;
4. participation in any of the actions under point 1 to 3, the association for the purpose of such an action, the attempt to do so, as well as the assistance, instigation, facilitation or counseling in the performance of such an act or its cloaking.

Money laundering s exist also when the above-mentioned activities have been performed in another Member State or in a third country and is not within the jurisdiction of the Republic of Bulgaria.

We are looking thorough the Country of Main Professional Activity of our customer. Therefore, as Country of Main professional activity is defined, the country from which:

i. Comes the main part (bulk) of the funds of the Customer,
ii. Where mainly operates as professional (the customer),
iii. Where the business transactions of the customer are carried out mainly, either directly or through partner(s),
iv. Where the Customer has an important political or entrepreneurial activity and presence (i.e. country in which it is considered as politically exposed person).
v. Caution: in case of offshore companies the above points (1) - (4) should be assessed in relation to the real beneficiary (Beneficial Owner).

vi. Indicative parameters for the assessment of the countries in which the customer operates, is also the country of residence and nationality of the Customer.

Under the principle «Know Your Customer» requires the continuous monitoring of the following:

i. The determination of the country's main business activity for each Customer, and

ii. The selection and classification of the most dangerous country (high risk, e.g. Not FATF countries), in which case the customer operates his main professional activities, when is more than one country.

iii. EXAMPLE- Customer located in Bulgaria, has been active in exports to Russia (which is directed toward the 1/3 of exports) and in China (where directed the 2/3 of exports). The countries of Russia and China are not included in non-high risk for ML. Between the two is selected as the country Main professional activity for the particular customer, China, as well as the customer develop toward this greater business activity.

4.3. Client authentication procedures and "know your client" (KYC) information

4.3.1. Profile Making

The identification of the customer (beneficial owner) must be carried out before entering into business relations and in any case before the conclusion of transactions and with the use of reliable third-party sources (third party diligence) which their data are hard to be falsified/ forge/faked.

By way of derogation- from the previous paragraph- shall be permitted to complete the verification of the identity of the customer (beneficial owner) when entering into business relations, where this is required, so as not, to, interrupt the smooth provision of services. However, even in this case, the risk money

laundering from criminal activities or terrorist financing must be small. In these cases, the proceedings are terminated as soon as possible after the initial contact, and in any case no later than 30 days. The data for the identification of the customers (true) identity as well as the process of opening a new customer's file is included, in the process of operations.

For the preparation of the profile of the customer, we request as minimum the following:

Customer Data:

- The description of the professional or business activity,
- The elements of the Group/ associated companies/the ownership structure and composition of shareholders, the country Headquarters of the Group / the associated companies,
- The real beneficiaries, historical data of growth, professional and operational activity,
- Assets size sources and assets and in general the economic background

Economic /Transactional profile:

- Real country of operations
- The purpose of the relationship and the business – financial services accounts,
- The nature of the requested STREAMFLOW EOOD int./ non-STREAMFLOW EOOD int. services,
- The planned movement of accounts, and money transferring
- The variety and the amount of trade,
- Country/countries of destination for outgoing transfers or payments,
- Reference to the risks that could result from the relation, example due to Country Risk, legal form, kind of transactions, services, and products, etc.

It should be noted that the data collection should be carried out considering comply with the principle of protection of personal data of the Customer.

4.3.2. Evaluation

A. For Recurrent – Business Customers- Partners

I. The company accepts the customer only where they do not belong to any of the categories of non-eligible customers. The verification of the customer is being carried out in accordance with the Operations procedures (registration process /Identification/Acceptance of prospective customer).

II. During the assessment of the customers, the policy of the company for the Money Laundering (from now ML) and (Financing Terrorism) (from now on FT) is taken seriously into account. Moreover, the risks involved and occur, from the operation of the company since the beginning of the relationship.

III. If, during the course of the cooperation, issues occur that are grounds for breaking off this cooperation and from the beginning rejection of the relationship for reasons ML and FT, the decision shall be communicated to the customer without mentioning the real reasons and inform immediately the MLRO.

IV. The company may revoke its decision on co-operation in case problems occur:
- During the stage of identification of the Customer
- During the presentation and control of legitimising documents
- During the relationship

4.3.3. Politically Exposed Persons

4.3.3.1. Politically Exposed Persons

In respect to identifying during the onboarding process whether a client is a PEP, the Company will:

1. Use Automated Compliance Screening database;

2. Ensure internal procedures include employee ongoing training programmes, addressing effective ways of determining whether clients are PEPs;
3. Use the Internet and media as a source of information for the determination, monitoring and verification of information in relation to PEPs;
4. Use countries' published lists of domestic PEPs; and
5. Use general information publicised by competent authorities (e.g. the level of corruption in the country, the level of income for certain types of positions).

Once a client is identified as a PEP, the following due diligence measures shall be applied:

1. The Company shall take adequate measures to establish the source of wealth and the source of funds to be used in the business relationship in order to ensure that it will not handle the proceeds from corruption or other criminal activity. The Company will verify the source of wealth and funds on the basis of reliable and independent data, documents or information;
2. Senior Management approval will be required for the establishment (and subsequently the continuance) of the business relationship. In this respect, the MLCO will provide a report to the Risk Committee that will confirm that the PEP client has provided all requested information / documentation. Once approval is granted by the Risk Committee, the MLCO must be notified. When considering whether to approve the relationship, the Risk Committee shall base its decision on the level of ML risk the Company will be exposed to by the relationship and how well equipped the Company is to manage the possible risk effectively;
3. The Company will conduct enhanced on-going monitoring of both transactions and the risk associated with the business relationship.

PEP Monitoring:

The accounts of PEPs shall be subject to on-going monitoring. At least an annual review shall be performed in order to determine whether to allow the continuance of operation.

In this respect, a short report shall be prepared summarising the results of the review by the MLCO. The report shall be submitted for consideration and approval to the Senior Management and filed in the customer's file.

The Company shall ensure that a client's due diligence information is kept up to date, as existing clients may sometimes become PEPs after the establishment of the business relationship. As part of this process, the Company will perform regular re-screenings via Compliance automated database screening to identity whether a PEP client maintains his PEP status or whether the status of a non-PEP client has changed.

In a case that a PEP is no longer entrusted with a prominent public function by a Member State or a third country, or with a prominent public function by an international organization, the Company shall, for at least 12 months, take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to PEPs.

PEP Registry:

The Company shall maintain a PEP's registry, which shall include the relevant details of the PEP with whom a business relationship has been established or rejected.

B. For non-Recurrent Customers (Physical Persons)

I. Non- recurrent is considered to be a customer, that is not strategically selected, as a business partner, all of the times it is a physical person, so there, limited KYC and AML Procedures do apply.

II. Non- Recurrent customers, are considered to be those customers (physical persons) that use STREAMFLOW EOOD' electronic of E-Voucher services, but the issuing of these vouchers is done by a third party (business partner/ customer) that goes through KYC procedures, within his own network and takes logical measures (Due Diligence Procedures).

III. For those customers, the strategic partner/ customer must demonstrate the KYC and AML Procedures that he performs in order for STREAMFLOW EOOD to obtain a third-party reliance upon the no-recurrent customer.

IV. Also, ***Business Partner/ Customer*** shall demonstrate the collection and verification of information and also identification of information, which is carried out, under specific thresholds. In any case, STREAMFLOW EOOD and the relevant MLRO officer or External Auditor has the authority to conduct audits to this matter.

V. When there are reasonable grounds for suspecting money laundering from criminal activities or financing of terrorism regardless of any derogation, exclusion or threshold amount (minimum threshold) of the transaction to be carried out, then we apply measures of due diligence independent from the amount of transaction, despite the measures that our business customer partner applied.

VI. The minimum data that our ***Business Customer/ Partner*** has to collect – regarding physical persons (**non-recurrent customers**) and people that are using STREAMFLOW EOOD' money transaction services (E-Vouchers) are the following,

In simplified Customer Due Diligence

Required information	Documents Required Certification
▪ Name- Surname ▪ Date –Place of birth ▪ Nationality ▪ Any citizenship that the person holds ▪ I.D. / Passport number ▪ Issuing authority ▪ Country of residency	An identity card or passport (or equivalent document) – valid- or identity card of Armed/ Security forces, which bring photo of the Customer.

In Normal and Enhanced Customer Due Diligence (most of the cases)

Valid (current) Home Address and contact phone	Utility +phone bill
Profession and current address of workplace	Copy of his employer, copy of last salary statement or beginning ca –tax office, professional identity or document of Social Security Institution.
Tax Identification Number	Photocopy of salary slip/ tax awareness document or utility account

Enhanced Customer Due Diligence is obligatory with respect to PEP irrespective they are potential clients, existing clients and actual owners of a client.

4.4. Business relationship & trade without physical presence of the Customer

Because of the nature of the object of our company, all transactions are carried out without the physical presence of the customer. Therefore, the same or additional measuresmay apply. Additional measures, such as:

- Client identification with additional supporting documents, data or information from valid reliable 3rd party sources.
- Ensuring that the first payment, within the framework of the business relationship, or any individual transactions, carried out through an account opened in the customer's name with a credit institution established in one of the Member States of the European Union or in a state with an equivalent supervisory regime and Controlling State Authorities.
- Countries characterised by the FATF or Bulgarian State Agency for National Security as "uncooperative" or the countries which do not apply or apply poorly the recommendations of the FATF, considered high-risk countries. There are no business relationships with natural or legal persons, including credit institutions

and financial institutions, which are derived or have establishment of headquarters in these countries. Transactions which may come/ result from these countries, regarding market products services that our customers' needs, shall be examined with particular attention and are subject to continuous monitoring.

4.5. Customer Data- Maintaining files

The completeness of the supporting documents that have been collected for the certification and verification of the identity of strategic customers and partners by STREAMFLOW EOOD, and on some and physical entities/ persons, is checked on the basis of the "Condition Required supporting Authentication Legal (and natural) Persons", by specific employees or the MLRO. This situation is part of the file each Customer. The file shall be maintained for 5 years and shall be accessible to Bulgarian State Agency for National Security during this period.

Also, we check the quality of the supporting documents, which must in any case be:

- Legible and readable
- Formal and official documents
- Valid at the beginning of the relationship

With respect to the certification of the identity of the legal persons or entities, the validity of legitimising the required documents shall be certified by the cooperating law consultant office/ employees of our company.

With regard to the legal persons established outside Bulgaria without installation in the country, the documents to be presented should be bearing the stamp Apostille and translated into officially Bulgarian language, if the company deems it necessary.

The identification of the customers, as well as the legal documents of companies should be checked annually and updated accordingly. The photocopies of the above documents authentication shall be kept for a period of at least five years after the end of the business

relationship, in such a way as to ensure the confidentiality of collected data. The financial transactions should be kept for ten years or as long as the EU and Local Legislation requires.

Responsible, for further communication with the Bulgarian State Agency for National Security or other competent State authority is the MLRO of STREAMFLOW EOOD. To perform this, STREAMFLOW EOOD perform the procedure to identify the beneficial owner. “Beneficial owner” refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.”

Identification of beneficial ownership:

- Data authentication of the beneficiaries of the account;
    - With respect to the natural person opening the account: name and title;
    - With respect to the legal entity customer: name and address;
    - With respect to the beneficial owners:
        - Name (and title for the controlling individual(s));
        - Date of birth;
        - Address; and
        - Social security number, Tax Identification number (TIN), or passport number and country of issuance or similar ID number.
- Data authentication of persons who have the right of controlling the account;
- Legal documents of all kinds legal entities/ persons;
- Data authentication of administrators and their legal representatives who are authorized to initiate and move the account of a legal person, legal documents and supporting documents of trade;
- Data relating to the volume and the transactions carried out by the means of account which indicates the
    - origin of the money;
    - Type and amount of currency of the transaction;

- The way in which the money deposited or taken, i.e. cash, electronic transfers etc.;
- Identity of the person who carried out the transaction;
- Destination of the money;
- Written approvals and authorisations of Customers;
- Type and number of account involved in the transaction.

- Certificate from the respective Trade Registry of other register, showing the beneficial owner.
- Declaration from the legal representative of the entity, revealing the beneficial owner.

Where identification procedures do not satisfy us as to the true identity of the customer the MLRO must be consulted to determine if the issues can be resolved. This is vital as consent from the authorities may be required before we proceed if we are to avoid being charged with non-compliance with applicable regulations.

4.6. Rating Strategic Customers/ partners

The company, for the identification and evaluation of the overall risk facing, take into account at least:

- The risk from the business/ professional activity of the customer (e.g. complex ownership structure legal persons, PEP, etc),
- The risk from the market behavior of the customer (e.g. difficulties in identifying the source and origin of the assets of the client, reluctance to disclose their real owners' legal person etc.),
- The risk from the products and services provided to the customer (e.g. web check out, mobile check out etc.),
- Country Risk (Origin, destination funds or carrying out work).

The factors (parameter) taken into account for the assessment and the classification of customers by degree of risk is:

A. Value Limits and Segmentation of services

Non-exclusive list of indicative criteria: transaction over EUR 15.000 shall be monitored, the threshold applies to a single transaction or to a series of consecutive transactions with some purpose or within short period of time.

B. Methods of funding

Non-exclusive list of indicative criteria:

2.1. (expected) incoming (and outgoing) flows of funds, including volumes, should be monitored;

2.2. the product; e.g. credit cards from high-risk countries, bitcoin, prepaid cards, e-wallets or PaypPl;

2.3. the use of different STREAMFLOW EOOD or credit card numbers for the initial purchase

C. Geographical limits

Non-exclusive list of indicative criteria:

2.4. the countries in which the customers have their clients, and from which transactions will therefore mainly originate (compliance with FATF and Bulgarian State Agency for National Security lists);

2.5. the transaction's country of origin or country of destination; e.g. high-risk country, EU or non-EU country;

2.6. payments from IP addresses in high-risk countries;

D. Usage Limits

Non-exclusive list of indicative criteria:

4.1. the types of transactions and their frequency (credit card, non-cash transfers, foreign currency, etc.)

4.2. the time lapses between purchase and payment, refunds or charge backs;

4.3. the time of the underlying transaction or transactions (transactions are for example conducted outside the opening hours of the payments terminal location;

4.4. he time periods between purchase and payment, refunds or charge backs;

4.5. the customer uses many different IP addresses;

4.6. multiple payments made at a particular merchant using credit cards with the same BIN from an exotic STREAMFLOW EOOD ;

E. Type of customer: e.g. PEP, the customer segment; e.g. gambling, gaming, erotic, charitable foundations, hospitality, online retailers with chemicals, online retailers selling anonymous phone and SIM cards, traders in gold, coins, bitcoin/crypto currency exchange, hosting services, administrative consultancies, consultancy, training and education, travel or crowdfunding; changes in transaction behavior which cannot be explained by the activities of the client;

As a result of this evaluation, the customers of the company are classified internally in three categories:

1. **High Risk** – at least 3 abovementioned factors reached.

By default, the following customers shall be treated as High Risk

- Legal persons established outside Single Economic Area and FATF offshore companies (Not Applicable)
- Legal persons or associations of persons non-profit-making body, trusting funds, institutions and accounts for third.
- PEP of third country. (Not Applicable).
- Customers operating in some of the classes which the company considers as high-risk.
- Customers based or activity in one of the countries which the company considers as increased risk each other case which is classified in this category by the responsible Compliance

2. **Medium Risk** – All the other cases which are not covered by as High Risk.

3. **Low Risk, the following clients:**

• Credit institution or financial institution of a Member State of the European Union, or a credit institution or financial institution which is situated in a third country which imposes requirements which are equivalent to those laid down in European Community legislation and is subject to supervision with respect to the compliance with these requirements,

• Company whose securities are admitted to trading on a regulated market in a Member State of the European Union or in a third country are subject to transparency requirements that are equivalent to those laid down by European Community legislation,

• National Public Authorities.

STREAMFLOW EOOD, carries out, periodic assessment clients from the Commercial Department for all customers. In addition, may hold an emergency assessment and customer accounts. The special assessment shall be carried out according to the criteria in the system. In particular, the emergency procedure evaluation is activated on the following cases:

- ✓ When the customer makes an important for him and for his profile transaction (if the average trade increased both in volume and value over 20 %.)
- ✓ When the customer may have high volume disputed transactions
- ✓ When there is a significant change in customer information (e.g. on the operations of the customer)
- ✓ When the company realized that lacks sufficient information for an existing customer or there are doubts as to the accuracy and adequacy of the data collected in the past.

For the purpose of calculating the limit of 15,000 euro will be taken into account all the transactions which it seems to have been a relationship between them according the Bulgarian AML Act and FATF regulations.

The above classification is carried out by means of a written risk analysis for each customer for the categories high and medium. For the customer of high-risk measures apply enhanced due diligence.

5. MYC- MONITOR YOUR CUSTOMER PROCEDURE

5.1. Continuous Monitoring of business relationship

The business relationships are monitored continuously, through the continuous examination of transactions and activities of the customer and the actual beneficiaries throughout the duration of the relationship.

If new information arises during the examination of the activities of the customer and the trade, from another unit of the Company or from independent sources which relate to the transaction or economic activity of the customer, then his profile shall be updated whenever the transactional/financial profile of the customer with care of the parties involved (Customer Relationship Officer, Commercial Address) and also reevaluate the relationship.

5.2. Document monitoring and Tracking

STREAMFLOW EOOD in addition of the responsibility of the collection and storage of the identity of clients, also has the responsibility of updating them throughout the duration of the business relationship and in particular when there are doubts about their validity. The verification of data shall be carried out on a periodic basis.

For the updating of the information letter is sent to the customer and the real beneficiary, in which all the data and documents in the possession of the company and calls for written confirmation on the accuracy and the validity of or send new updates supporting documents, in case of changes. The file of each customer is kept and all documents of reference samples shall be taken.

The MLRO reviews on a periodic basis the completeness of files of customers, the updating and the compliance with the current procedures. In case that it is not possible to update the authentication of the client, shall be informed the Customer Relationship Officer for further action with the Customer. If difficulties arise with regard to updating of the data, it is possible that:

a) We terminate the relationship

β) Submission of confidential reporting suspicious transactions to the corresponding AML State Authority, where there are visible signs of ML and FT.

5.3. Monitoring of accounts & transactions

STREAMFLOW EOOD continuously monitors the accounts and transactions of customers for the effective treatment of risk ML and FT, through to identify unusual or suspicious transactions.

For example, controlled the nature of each individual transaction irrespective of the amount involved e.g. the category of financial instrument, the frequency of transactions, the complexity, the country of destination, the origin, if there is sufficient justification and whether it is compatible with the nature of the transaction, etc.

In any case, the transfer of funds shall be made into an account payment which has been opened and maintained by the customer in an approved credit institution within the EU.

5.4. Record Keeping Requirements

The MLCO must maintain a registry of all information received from employees regarding transactions of money laundering or terrorist activities and the decision of whether to report or not the complaint to MOKAS.

Records of all documents/data in relation to suspicions of ML/TF will be maintained for a period of at least 5 years which is calculated after the execution of the transactions or the termination of the business relationship.

The documents/data relevant to ongoing investigations will be kept until MOKAS confirms that the investigation has been completed and the case has been closed.

The documents should be kept in a hard copy form, in their original or in a certified true copy form. A true translation should be attached in case the documents are not in the Greek or English language.

5.5. Right of Audit and Suspicious Activity Reporting (SAR)

STREAMFLOW EOOD will ensure that all customer identification documentation is safe and is forwarded to local authorities, in a timely manner, only upon request. The STREAMFLOW must ensure that all members of staff are aware of their personal obligations under the Bulgarian AML Act 2018, to promptly raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds to have knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists. The MLRO receives any internal reports and is responsible for reporting to the Bulgarian State Agency for National Security, if he considers a suspicious activity report is deemed appropriate.

6. PROHIBITED COUNTRIES/INDUSTRIES LIST

STREAMFLOW List of Prohibited Businesses
Customers or Endusers cannot be conducting the below types of businesses.

Streamflow Prohibited Business	Type	Risk Level
Cryptocurrency trading	Crypto	Prohibited
Anonymous or Numbered Accounts, Shell Banking	Financial Services	Prohibited
Cash and Cheque Handling: Cheque Cashing, Deposit Taking, Cash Transfer,	Financial Services	Prohibited
Credit repair, Debt Restructuring,	Financial Services	Prohibited
Debt recovery, Debt settlement, Debt Collections,	Financial Services	Prohibited
Financial Pyramid or Ponzi Schemes	Financial Services	Prohibited
Gambling and Gaming	Financial Services	Prohibited
MSBs and PSPs as endusers (with Railsbank approval only)	Financial Services	Prohibited
Any industry known to be an illegal industry in it's local jurisdiction or the UK	Illegal Services	Prohibited
Illegal Drugs and Narcotics	Illegal Services	Prohibited
The sale or distribution of stolen goods (including digital and virtual goods), counterfeit goods and violation of intellectual property, or items that violates individual privacy (revenge porn)	Illegal Services	Prohibited
Any products harmful to human health - tobacco, e-cigarettes and e-liquid (pharmacological products are subject to Railsbank approval)	Other Services	Prohibited
Operating a business that requires a license or special permit without obtaining such license (i.e. Unregulated Auction Houses)	Other Services	Prohibited

Production of Adult or Violent content	Other Services	Prohibited
Production or Distribution of Offensive Weapons: Ammunition, Firearms, Explosives, Complex Weapons (i.e. guided missiles), Poisons	Other Services	Prohibited
Psychic services	Other Services	Prohibited
Selling, hosting, distributing, producing or promoting offensive materials, including materials that incites or promotes racial hatred or discrimination based on gender, race, religion, national origin, physical ability, sexual orientation, or age	Other Services	Prohibited
Transactions involving Human Organs	Other Services	Prohibited
Sanctioned individuals and entities	Sanctions	Prohibited

Streamflow List of Prohibited Jurisdictions

Customers and Endusers cannot operate within these jurisdictions or send/receive money to these jurisdictions.

Country	Country Code	Risk Bracket
Afghanistan	AF	Sanctioned
Crimea	N/A	Sanctioned
Cuba	CU	Sanctioned
Iran, Islamic Republic of	IR	Sanctioned
North Korea	KP	Sanctioned
Syria	SY	Sanctioned
Venezuela	VE	Sanctioned
Belarus	BY	Prohibited

Central African Rep	CF	Prohibited
Congo, the Democratic Republic	CD	Prohibited
Eritrea	ER	Prohibited
Ethiopia	ET	Prohibited
Guinea	GN	Prohibited
Iraq	IQ	Prohibited
Lebanon	LB	Prohibited
Liberia	LR	Prohibited
Libya	LY	Prohibited
Mali	ML	Prohibited
Myanmar	MM	Prohibited
Pakistan	PK	Prohibited
Russian Federation	RU	Prohibited
Somalia	SO	Prohibited
South Sudan	SS	Prohibited
Sudan	SD	Prohibited
Ukraine	UA	Prohibited
Yemen	YE	Prohibited
Zimbabwe	ZW	Prohibited