RISK MANAGEMENT POLICY (AML POLICY)

Swapster warns Users against attempts to use Swapster for money laundering, legalization of funds obtained by criminal means, purchasing prohibited goods and services, terrorist financing, fraud and any other illegal activities. Swapster also warns Users against attempts to conceal information linking them to individuals and legal entities, organizations or countries included in the sanctions lists of the Russian Federation.

The Risk Management Policy (hereinafter referred to as the “Policy” or “AML Policy”) sets up control systems and mechanisms to prevent the involvement of Swapster's company and its services in money laundering, terrorist financing activities and violation of established sanctions restrictions. The policy also defines rules for preserving and maintaining the reputation of Swapster when interacting with Users, counterparties and representatives of authorized bodies.

Under this Policy, the words "Swapster website", "we", "us" or "our" refer to Swapster, including all of its employees and other related persons. Depending on the context, "Swapster" may also refer to services, products/goods, website, content or other materials provided by Swapster. The Policy is an integral part of the Terms of Use. By accepting the Terms of Use, the User automatically agrees to this Politics.

Before using the Website or any other service offered on the Website and/or by Swapster, the User should carefully read this Policy. In case of disagreement with any part of this Policy, Swapster kindly asks the User not to use the Website and its services.

1. DEFINITIONS

All terms in capital letters specified in this AML Policy that are not otherwise defined have the same meaning as in the Terms of Use.

Swapster – in this Risk Management Policy (AML Policy) *Swapster* shall mean MARKETING TECHNOLOGY IT DEVELOPMENT LLC, a legal entity registered on 10/06/2022 under the law of Georgia, with identification code: 422941473, having a legal address at Georgia, Tbilisi, Gldani District, Omar Khizanishvili Street, №264 (Free Industrial Zone of Tbilisi Technology Park);

Definitions — terms in capital letters and in this Policy having the meanings specified in this section.

Legalization of proceeds of crime – concealing the illegal source of funds by transferring them into money or investments that appear to be legitimate.

Prohibited Conduct – any illegal behavior that includes fraud, corruption, money laundering, conspiracy, terrorist financing and any other criminal behavior.

Fraud – use of deception to pursue personal interests and to damage the interests of Users and/or Swapster by stealing or acquiring the right to another's property by deception.

Deception – a method of fraud to receive money from Internet users, which may include withholding information or providing incorrect information in order to extort money, property and inheritance from victims.

Corruption – offering, giving, receiving, or soliciting, directly or indirectly, anything of value that would improperly influence the actions of another party.

Client (User) — an individual visiting the Website https://swapster.fi and/or using the Services to receive the services of the Website and Swapster Services and being a data subject and/or Client.

Money laundering – a financial transaction scheme aimed at concealing the identity, source and destination of illegally obtained money or financing illegal activities.

Anti Money laundering (AML) – a set of measures and procedures aimed at detecting and/or preventing the use of Swapster and/or the services provided by Swapster for money laundering purposes.

Counter-terrorist financing (CTF) – a set of measures and procedures aimed at detecting and/or preventing the use of Swapster and/or the services provided by Swapster for terrorist financing purposes.

Sanctions (economic sanctions) – commercial and financial sanctions applied by one or more countries against targeted self—governing states, groups or individuals.

Red flags – warnings or indicators suggesting that there is a potential problem or threat with Users' transaction that goes through Swapster and/or the Swapster's Service, Website.

Website – https://swapster.fi/.

Conspiracy – an agreement between two or more parties aimed at achieving an improper goal, including undue influence on the actions of the other party.

Terrorist financing – provision or collection of funds by any means, directly or indirectly, with the intention of using them or on condition that they will be used in whole or in part to carry out any of the crimes/operations related to terrorism.

Criminal conduct – a crime, or an action that would qualify as a crime in any part of the world.

Know Your Client (KYC) – a set of measures and procedures aimed at obtaining information about the User and his/her activities in order to manage the company's risks.

Client Due Diligence (CDD) — verification of data/information about the User and other checks related to the study of the User and his/her activities. CCD is conducted for the purpose of a comprehensive risk assessment of the User when onboarding him/her for service, or when providing services to him/her.

Politically exposed person (PEP) – an individual who has a prominent public role within a country or internationally.

Regulatory Requirements — any applicable law, statute, regulation, order, judgment, decision, recommendation, rule, policy (including but not limited to AML Policy) or guideline. They must be adopted or issued by the Parliament, the government, any competent court, authority, a payment system. This includes bank payment systems, card payment systems or any other payment, clearing or settlement systems, or similar agreements that are used to provide the Services.

Policy/-ies — Policies, regulations, Agreements governing the provision of Services, including, but not limited to Risk Management Policies, Confidentiality policy and similar documents and regulations.

2. GENERAL PROVISIONS

2.1. This Policy sets out main standards, principles, rules and approaches used by Swapster to study sanctions and countries, as well as its Users and counterparties, carrying out measures to manage the risks of money laundering and terrorist financing.

2.2. Internal documents on AML/CTF risk management and KYC/CD procedures are developed by Swapster additionally and are confidential information of Swapster with limited access. Such documents comply with this Policy.

2.3. Swapster ensures compliance with the requirements of this Policy and applicable legislation by all Swapster employees.

2.4. In order to provide an appropriate and timely level of services to Users, Swapster and its Users are required to comply with the requirements contained in domestic and international laws on the prevention of money laundering and terrorist financing, as well as the requirements of other laws and regulations to the extent that they are related to the activities of Swapster.

2.5. In order to carry out the procedures provided for in this Policy, Swapster develops and implements an internal system for assessing the level of risks of the User and their operations. It also defines the minimum required set of requirements, procedures, mechanisms, reports, systems and controls for Swapster risk management. Stricter procedures are applied for high-risk Users and transactions.

2.6. Swapster may make changes and additions to the Policy unilaterally and at its own discretion as new risks are identified, new products/services are introduced and changes in the applicable legislation are made, as well as monitor compliance with its provisions and requirements.

3. KYC PROCEDURES

3.1. Swapster conducts a KYC verification procedure to avoid the risk of being held liable for violating applicable laws, as well as in order to protect itself from attempts to use Swapster and/or its services to conduct illegal activity.

3.2. Within the KYC procedure Swapster:

3.2.1. establishes the identity of the User — studies the User when onboarding and clarifies information about him/her during the services provision.

Swapster performs identification procedures related to the User:

a) when onboarding/registering of a User;

b) annually for high-risk Users, every two years for medium-risk Users, every three years for low-risk Users;

3.2.2. examines the nature of the User's activity — the User's transactions in order to assess the money laundering risks associated with this User. The main goal is to make sure that the source of funds is legitimate;

3.2.3. collects and stores information about Users, the results of their review, as well as about material facts concerning existing and potential Users and their transactions.

3.3. In order to identify Users, Swapster may request the following documents:

3.3.1. For individuals (depending on the type of product or access to products and services):

<u>contact information:</u>

- nickname in the messenger (Telegram);
- phone number;
- Email address.

<u>identification documents:</u>

- domestic and/or foreign passport;
- ID card;
- driver's license.

<u>confirmation of address of residence/registration:</u>

- a copy of the utility bill;
- a copy of the phone bill;
- a copy of the electricity bill;
- bank statement.

other documents if necessary.

3.4. Comprehensive Users’ verification.

In the process of studying/reviewing Users, Swapster can perform three levels of verification:

● Simplified Due Diligence ("SDD") —when the risk of money laundering or terrorist financing is low and full verification is not required. Example: accounts with low turnover and transaction amounts.

● Basic Client Due Diligence ("CDD") — information received from all Users to verify the identity of the User and assess the risks associated with this User.

● Extended Due Diligence ("EDD") — additional information collected about higher-risk User for a deeper understanding of the activities of such User and to reduce the risks associated with them.

3.5. The onboarding/registration of PEP as a User takes place only after Swapster Management’s approval. Those type of Users are to be considered high-risk and the EDD procedure shall be applied to them.

3.6. After carrying out identification procedures related to the User, Swapster stores the information received in the file of this User.

3.7. Swapster strives to protect the rights of Users and the confidentiality of their personal data. Swapster collects personal information from Users only to the extent necessary to ensure the proper provision of services to Users. Such personal information about Users and former Users may be transferred to third parties only under a limited number of circumstances in accordance with applicable law and/or requests from competent authorities or in accordance with the procedure provided for in the Terms of Use and/or Privacy Policy.

3.8. Swapster carefully stores the User's files, including statements, transaction reports, receipts, notes, internal correspondence and any other documents related to the User, in electronic format for the required time. They can be requested by compliance teams in the relevant acquiring banks/processors used by the User, payment agents involved in transactions, law enforcement agencies and/or other government authorized bodies, etc.

3.9. Swapster has the right to suspend an Account related to suspicious activity, including, but not limited to, activities that can be defined as money laundering, terrorist financing, fraud, etc.

Swapster has the right to ask the owner of such an Account to undergo an in-depth KYC procedure (provide additional necessary documents). If the User does not provide the necessary documents, or the documents provided are insufficient to remove suspicion of such activity, Swapster has the right to suspend the service of the User's account/operations temporarily or indefinitely, including until the account is completely blocked and all assets are blocked.

3.10 Swapster reserves the right to receive additional information about Users who have been identified as High-risk Users. Also, if the identification information has been changed, or the User's actions seemed suspicious to Swapster, the latter has the right to request documents from the User again, even if the User has already passed the verification earlier.

4. SUSPICIOUS ACTIVITIES DETECTION

4.1. Any financial transaction that may be related to money laundering, terrorist financing, violation of sanctions restrictions, fraud is considered suspicious.

4.2. Swapster independently develops and implements a mechanism for identifying such operations, a Red flags detection system, criteria for determining risks. The basis for determining that a particular transaction is suspicious may be personal observations and the experience of Swapster employees, information obtained during KYC procedures, information, obtained using specialized analytical programs and/or systems, etc.

4.3. Swapster regularly monitors the transactional activity of its Users. Swapster updates the Red flags systems and criteria used to detect suspicious activity and implements best international practices for detecting suspicious activity.

4.4. In accordance with applicable law and requirements of competent international bodies, Swapster may notify regulatory and/or law enforcement authorities of any suspicious transactions, as well as provide the necessary information in response to requests from such organizations and bodies. Swapster may act where appropriate and has no obligation to obtain User’s approval or to notify them.

4.5. When reviewing Users and analyzing their transactions, Swapster uses the following:

- list of sanctioned persons, known terrorists and/or terrorist organizations, as well as persons suspected of terrorist activities. The lists should be published by local authorities and international organizations: OFAC (Office of Foreign Assets Control), EU, UN, etc.;
- list of jurisdictions that do not provide a sufficient level of anti-money laundering procedures in accordance with FATF policies, as well as countries subject to OFAC, EU, UN and other sanctions;
- list of high-risk jurisdictions and territories *(Appendix 1)* to determine whether a Swapster User or a potential User and/or the countries or jurisdictions of such a User are included in the above lists, cooperation with which is prohibited or undesirable.

4.6. Swapster constantly checks and reviews its Users and verifies their transactions to ensure that these transactions are compatible with Swapster's data about its Users, their business and, if necessary, their sources of income.

4.7. Swapster does not establish relations with Users who are included in the sanctions lists, registered/located in the territories/jurisdictions specified in clause 4.5. or are under the control of such persons.

4.8. If the User has extremely high-risk status, Swapster may refuse to provide such a User further service.

4.9 If suspicious transactions are detected, Swapster also reserves the right to request additional documents from the User, suspend or terminate the User's account, suspend turnover or freeze the User's assets. The suspension lasts until the circumstances and other actions commensurate with the identified risks are clarified.

5. THIRD PARTIES

6.1 Swapster may engage third party service providers or interact with counterparties to perform some of its business functions. Swapster makes every effort to review such service provider/contractor and its activities and to determine, to the extent possible, its reputation (whether there are any initiated investigations and lawsuits against any such third-party service providers). Swapster also determines whether the third-party provider has obtained all necessary licenses, permits and approvals before establishing a business relationship with such third-party service provider.

6.2 Swapster shall not establish a relationship with a service provider and/or counterparty that is on the sanctions lists or registered/located in the territories/jurisdictions referred to in clause 4.5 or that is under the control of such persons.

6. EMPLOYEES AND REPRESENTATIVES TRAINING

6.1. Swapster takes all possible measures to train employees in order to prevent Swapster from being involved in actions aimed at using Swapster and/or Swapster's services for the purpose of money laundering, terrorist financing, fraud or violation of set sanctions restrictions.

6.2. In regard to its own employees/staff, Swapster takes all possible measures to thoroughly analyze and review all job candidates in order to determine whether the activity and/or reputation of the new employee falls into a category that is subject to or carries money laundering risks.

7. SUSPICIOUS TRANSACTIONS AND HIGH-RISK USERS REPORTS

7.1. Swapster develops and implements internal report system that allows to receive timely information about Swapster risks and their management. If a Swapster employee becomes aware of an activity that falls under the restrictions specified in the Policy, the employee must immediately notify about that and provide all necessary available information to his/hers supervisor and/or authorized department (compliance) and/or senior management of Swapster.

8. USER AGREEMENT

8.1. By using the Swapster's products/services, the User warrants that he/she does not intend to engage in any of the prohibited activities described herein. In addition, the User consents to any inspections/reviews related to an investigation under the AML/KYC Policy and agrees to cooperate with the Anti-Fraud Commissioner, Verifier and other authorized persons fully and promptly in such investigation. Failure to cooperate or provide required information/documentation may serve as a ground for suspension of the User's service or refusal of further service altogether.

9. THE SWAPSTER'S EMPLOYEE RESPONSIBLE FOR COMPLIANCE WITH THE POLICY

9.1. The employee responsible for compliance with the Policy must carry out the following procedures:

- collecting Users identification information and transferring it to the responsible personal data processing agent;
- creating and regularly updating Swapster's internal policies and procedures required in accordance with existing laws and regulations;
- transaction monitoring and analysis of any significant deviations from normal User activity;
- initiate interaction with state and law enforcement agencies of countering money laundering money laundering, terrorist financing and fraud, if necessary.

10. MISCELLANEOUS

10.1. This Policy has been approved in the manner set by Swapster and approved by Swapster's Management.

10.2. This Policy comes into force from the moment of approval and/or publication on the Swapster's Website.

10.3 This Policy is publicly available on the Website in the current version. Swapster reserves the right to make changes to this Policy unilaterally.

APPENDIX No. 1

LIST OF RESTRICTED JURISDICTIONS AND TERRITORIES

cooperation is prohibited due to a high level of risk or for other reasons

1. American Samoa
2. Afghanistan
3. Bahamas
4. Botswana
5. Burma
6. Ethiopia
7. Crimea
8. Cuba
9. Canada
10. Republic of Ghana
11. Island Guam
12. Iran
13. Iraq
14. Yemen
15. Libya
16. Malaysia
17. Nigeria
18. Republic of Nicaragua
19. Singapore
20. North Korea
21. Pakistan
22. Panama
23. Puerto Rico
24. Sri Lanka
25. Somali
26. Saudi Arabia
27. United States of America
28. Republic of South Sudan
29. Republic of Sudan
30. Syria
31. Republic of Trinidad and Tobago
32. Transnistria, Pridnestrovian Moldavian Republic (PMR)
33. Tunisia Virgin Islands
34. Bolivarian Republic of Venezuela
35. Republic of Artsakh