**Anti-Money Laundering Policy (Anti-Money Laundering Policy).**

SolidSwap warns users against attempts to use the service to legalize criminally obtained funds, terrorist financing, illegal actions of any kind, as well as from using the service to purchase prohibited goods and services.

The legalization of funds obtained by criminal means is the concealment of an illegal source of funds by transferring them into funds or investments that look legitimate.

**General provisions**

To prevent illegal transactions, the Service sets certain requirements for all Applications created by the User:

* The sender and the recipient of the Payment on the Application must be the same person. Transfers in favor of third parties are strictly prohibited using the services of the Service.
* All contact information entered by the User in the Application, as well as other personal data transmitted by the User to the Service, must be up-to-date and completely reliable.
* It is strictly prohibited for a User to create Applications using anonymous proxy servers or any other anonymous Internet connections.

This Anti-Money Laundering Policy (hereinafter referred to as the "AML Policy") describes the procedures and mechanisms used by SolidSwap to counter money laundering SolidSwap adheres to the following rules:

* not to enter into business relations with known criminals and/or terrorists;
* not to process transactions that are the result of known criminal and/or terrorist activities;
* not to facilitate any transactions related to known criminal and/or terrorist activities;
* has the right to restrict or prohibit the use of all or part of the services for persons subject to restrictions: any US persons and/or any individuals included in the List of Citizens of Special Categories or Blocked Persons of the US Treasury Department, Consolidated Lists of EU Financial Sanctions or UK Sanctions Lists, as well as citizens and residents from limited jurisdictions, such as: United States of America, Afghanistan, Bosnia and Herzegovina, Democratic People's Republic of Korea, Democratic Republic of the Congo, Eritrea, Ethiopia, Guyana, Iran, Irhas the right to restrict or prohibit the use of all or part of the services for persons subject to restrictions: any US persons and/or any individuals included in the List of Citizens of Special Categories or Blocked Persons of the US Treasury Department, Consolidated Lists of EU Financial Sanctions or UK Sanctions Lists, as well as citizens and residents from limited jurisdictionsch as: United States of America, Afghanistan, Bosnia and Herzegovina, Democratic People's Republic of Korea, Democratic Republic of the Congo, Eritrea, Ethiopia, Guyana, Iran, Iraq, Lao People's Democratic Republic, Libya, Somalia, Sri Lanka, Sudan, Syria, Trinidad and Tobago, Tunisia, Uganda, Vanuatu, Ukraine, United Kingdom, Mainland China, Singapore, Hong Kong, Canada, Cuba, Uzbekistan, Crimea, France, Sevastopol, Donetsk and Lugansk regions.

**Verification procedures**

SolidSwap service establishes its own verification procedures within the framework of anti-money laundering standards - the "Know Your Customer" (KYC) policy.

* SolidSwap Service users undergo the verification procedure (provide a government identification document: passport or identification card). SolidSwap reserves the right to collect User identification information for the purposes of implementing the AML Policy. This information is processed and stored strictly in accordance with SolidSwap's Privacy Policy and Personal Data Processing Policy.
* SolidSwap Service can also request a second document to identify the User: a bank statement or utility bill no older than 3 months, which indicates the User's full name and his actual place of residence, the service also has the right to request photo/video verification of the client, if there is suspicion of dishonesty of the information provided.
* SolidSwap service verifies the authenticity of documents and information provided by Users and reserves the right to receive additional infervice verifies the authenticity of documents and information provided by Users and reserves the right to receive additional information about Users who have been identified as dangerous or suspicious.

If the User's identification information has been changed or his activity has seemed suspicious, the SolidSwap Service has the right to request updated documents from the User, even if they have been authenticated in the past.

**Responsible for compliance with the AML Policy**

The person responsible for compliance with the AML Policy The person responsible for compliance with the AML Policy is an SolidSwap employee whose responsibilities include ensuring compliance with the AML Policy, namely:

* collecting User identification information and transferring it to the responsible personal data processing agent;
* Creation and updating of internal policies and procedures for writing, reviewing, submitting and storing all reports required in accordance with existing laws and regulations;
* transaction monitoring and analysis of any significant deviations from normal User activity;
* implementation of a records management system for storing and searching documents, files, forms and journals;
* regular updating of the risk assessment.

The person responsible for compliance with the AML Policy has the right to interact with law enforcement agencies that are engaged in preventing money laundering, terrorist financing and other illegal activities.

**Transaction monitoring**

Monitoring User transactions and analyzing the received data is also a tool for risk assessment and Monitoring User transactions and analyzing the received data is also a tool for risk asses detection of suspicious transactions. If money laundering is suspected, SolidSwap controls all transactions and reserves the right to:

* report suspicious transactions to the relevant law enforcement agencies;
* ask the User to provide any additional information and documents;
* suspend or terminate the User account;
* suspend the exchange and freeze assets until the circumstances are clarified;
* return the funds to the user by canceling the exchange procedure, according to the user agreement;
* risk assessment.

The above list is not exhaustive. The AML Policy Officer monitors User transactions on a daily basis to determine whether