ANTI MONEY LAUNDERING POLICY

Last updated on 23 June 2023.

ROVI Money is a technology solution provider and provides crypto wallet to users. ROVI money also lets users deposit fiat and purchase cryptocurrencies with the help of 3rd party providers. ROVI Money is committed to the highest standards of Anti-Money Laundering (“AML”) and Counter-Terrorist Financing (“CTF”) compliance. Our robust compliance system is designed to comply with applicable law. This Anti-Money Laundering Policy (“AML Policy”) establishes a framework to identify, detect, tackle and mitigate risks of the payment gateway being used to facilitate financial crime.

This AML policy applies to all employees, officers, directors, third-party vendors, users, customers and other legal entities or persons associated with the functions and Our operations.

Words capitalized but not defined shall adopt the meaning prescribed under the Terms of Service or Privacy Policy. If not defined in the referred policies, such capitalised terms shall adopt the meaning under applicable law.

PLEASE READ THIS POLICY CAREFULLY BEFORE ACCESSING OR USING OUR PLATFORM OR ANY PART THEREOF. BY ACCESSING OR USING ANY PART OF THE PLATFORM, YOU AGREE TO BE BOUND BY THIS AML POLICY. IF YOU DO NOT AGREE TO THE TERMS OF SERVICE, PRIVACY POLICY AND/OR THIS AML POLICY, THEN YOU MAY NOT USE ANY SERVICES PROVIDED BY US. YOU MAY AVAIL THE SERVICE AT YOUR OWN RISK ONLY IF THE TERMS OF USE, PRIVACY POLICY AND THE AML POLICY OF THE COMPANY ARE ACCEPTABLE TO YOU. TABLE OF CONTENTS

1. Principles

We shall ensure that:

1.1 All our operations comply with the relevant legal requirements and regulations of the jurisdiction in which we operate.

1.2 We conduct regular risk assessments to identify and understand the risks of money laundering, terrorist financing, and proliferation financing associated with our customers and our platform.

1.3 We have implemented effective and appropriate anti-money laundering (AML) procedures, which are continuously monitored for their effectiveness.

1.4 We take all necessary measures to prevent the use of ROVI Money for facilitating or enabling money laundering or terrorist financing.

1.5 We fully cooperate with law enforcement agencies in their efforts to combat financial crimes, including money laundering and terrorist financing.

2. USER'S OBLIGATIONS

2.1. By accessing, downloading, or using the Platform, users acknowledge and agree that they are prohibited from using the Platform in any manner that violates the Platform's Terms of Service, Privacy Policy, AML Policy, or any applicable laws. Users also consent to any changes made by us to these policies without prior notice.

2.2. Users acknowledge and agree that all information submitted to us during the use of the Platform must be true, accurate, and complete. Any information or identification documents provided must belong to the user submitting them.

2.3. If there is a change of address, users are required to promptly notify us and provide updated proof of address within 6 months of making the address change.

2.4. Users are strictly prohibited from engaging in any Suspicious Transaction or Money Laundering activity, or conducting transactions with individuals listed on the Sanctions List. The Sanctions List refers to lists of natural and legal persons designated by countries, governments, international authorities, including entities such as the US

Department of the Treasury's Office of Foreign Assets Control (OFAC), the European Union, Monetary Authority, Monetary Authority of Singapore, and other applicable laws. A "Suspicious Transaction" refers to a transaction that, in good faith:

● Give rise to a reasonable ground of suspicion that it may involve proceeds of an offense specified under the Anti Money Laundering laws, regardless of the value involved; or
● Appears to be made in circumstances of unusual or unjustified complexity; or
● Appears to have no economic rationale or bona fide purpose; or
● Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

2.5 We reserve the right, at our sole discretion, to block, restrict, or terminate access to any user's account if we discover or suspect that the user is engaged in illegal activities.

3. CUSTOMER DUE DILIGENCE

3.1. KYC: We understand that there could be potential misuse of our Platform by state and non-state actors for money laundering, terrorist financing, and proliferation financing. To mitigate these risks and ensure compliance with applicable Anti-Money Laundering (AML) laws, we have implemented an identity verification process that requires users to provide government-issued identity cards or other officially recognized valid documents. All collected information will be processed in accordance with our Privacy Policy, which can be found here.

3.2. In line with the above and as required by applicable law, we have implemented a two tier-tier Know Your Customer (KYC) system as part of Customer Due Diligence (CDD):

3.2.1. Basic KYC: Any user who wants to do any Fiat transaction in the system excluding selling or buying of crypto needs to do basic KYC. At this level, users are required to

> Provide their phone number and enter the One-Time Password (OTP) sent to their phone

> Submit a valid government-issued identity card (Proof of identity).

We collaborate with third-party vendors to verify the user's details by comparing the provided data with relevant government databases.

3.2.2. Full KYC: All platform users who do any buying or selling of crypto need to do full KYC. Based on monthly transactions, users may need to complete Full KYC. At this level,

users must have already completed Basic KYC and additionally undergo video KYC, as well as submit documents as proof of the source of funds.

3.3. The information provided during KYC will be verified by our compliance team throughout the user's interaction with the Platform. To maintain updated user information and perform random checks, users may be required to undergo any KYC process at any given time. In such cases, users may be requested to submit additional documents, which may include, but are not limited to, income tax return forms or bank account statements. All requested and collected information will be stored and processed according to our Privacy Policy, available here.

3.4. All submitted user identity documents must be in English. If the document is not in English, please provide a translated and duly notarized version by authorized agencies.

3.5. Please note that the deployed KYC system may vary based on applicable laws and jurisdictions. As part of CDD, we take steps to verify the authenticity of the documents submitted by users. We reserve the right to investigate users who are deemed risky or suspicious. Additionally, we reserve the right to request up-to-date documents from users, even if they have previously passed the identity verification process. All collected information will be processed and stored in accordance with our Privacy Policy, available here.

4. ENHANCED DUE DILIGENCE (“EDD”):

4.1. Enhanced Due Diligence (EDD) measures are implemented for complex transactions, unusually large transactions, unusual transaction patterns, and users categorized as high risk. High-risk customers/users may include politically exposed persons (PEPs) or individuals from high-risk jurisdictions. EDD measures involve obtaining additional information or verification, increasing monitoring efforts, and restricting certain types or volumes of transactions. These measures are applied proportionate to the assessed risk. To ensure proper deployment of EDD, we undertake the following activities:

4.1.1. Regularly reviewing customers' profiles and transactions.

4.1.2. Gathering information about the user from available sources.

4.1.3. Conducting independent inquiries into the details provided by the user.

4.1.4. Consulting credible databases and other relevant sources.

4.2. We are strictly prohibited from engaging in transactions with individuals, companies, or countries listed under prescribed sanctions. We screen against the sanctions lists published by entities such as the United Nations, Financial Action Task Force, European Union, UK Treasury, and US Office of Foreign Assets Control (OFAC) in all jurisdictions where we operate. If suspicious transactions are identified, we may report them to the appropriate authority. Any disclosure to competent authorities will be treated with strict confidentiality in accordance with applicable rules and regulations. For more information on how we collect, process, and store information, please refer to our Privacy Policy available here.

4.3. In the case of foreign politically exposed persons, in addition to conducting Customer Due Diligence (CDD) measures, we ensure that:

4.3.1. We have suitable risk management systems in place to identify if a customer is a politically exposed person.

4.3.2. Senior management approval is obtained before establishing new business relationships (or continuing existing ones) with politically exposed persons.

4.3.3. Reasonable measures are taken to determine the source of wealth or funds.

4.3.4. Enhanced ongoing monitoring is conducted for the business relationship.

5. MONITORING TRANSACTIONS

5.1. We will monitor all customer transactions for any unusual or suspicious activities. The level of monitoring will be determined based on factors such as each user's risk profile. Our Compliance Officer will review and investigate any transactions that raise suspicion. If there is a suspicion, detection, or attempted suspicious transaction involving proceeds, it may be reported to the appropriate and competent authority in accordance with applicable law.

5.2. During regular checks, if we have reason to believe that transactions are linked to money laundering, terrorist financing, or any other illegal activity, we may request information to verify the customer's identity. By accessing, downloading, or using the Platform, users acknowledge and agree to cooperate fully with us in any inquiry, investigation, or direction from a competent law enforcement authority.

6. RISK ASSESSMENT

6.1. We have implemented a risk-based approach to combat money laundering and terrorist financing in compliance with relevant laws. To address the applicable risks, we classify our users into high-risk, medium-risk, and low-risk categories. The risk assessment takes into account various factors, including but not limited to:

6.1.1. Adequacy and completeness of user-provided identification information.

6.1.2. User's geographical location.

6.1.3. Users involved in highly complex or high-value transactions.

6.1.4. Users conducting transactions with or within jurisdictions known for high-risk activities.

6.1.5. Countries subject to sanctions, embargoes, or similar measures.

6.1.6. Countries identified by reliable sources to have significant levels of corruption or criminal activities.

6.1.7. Countries or geographic areas known to provide funding or support for terrorist activities or host designated terrorist organizations.

6.1.8. Financial or social status of the user.

6.1.9. Nature of the user's business activities and the regularity or duration of the business relationship.

6.1.10. Guidance provided by governmental and intergovernmental organizations.

6.2. All information related to a user's risk profile is treated as strictly confidential. The data collected for risk profiling is processed and stored in accordance with our Privacy Policy. Any disclosure of confidential information will only occur in compliance with the Privacy Policy.

6.3. Based on a user's risk profile, we retain the sole discretion to impose restrictions, suspend activities, or terminate operations if they contravene applicable law.

7. RECORD KEEPING

The information we gather, handle, and store will adhere to our Privacy Policy. Any data collected will be retained for a duration as mandated by relevant laws. If there is no specific timeframe specified by the applicable law, we will keep your information for a period of 5 years.

8. EMPLOYEE TRAINING AND AWARENESS

Our staff members undergo regular training to ensure a comprehensive understanding of our AML Policy and their respective AML-related responsibilities. These training programs are regularly updated to align with changes in regulations and our business operations. The goal is to equip our staff with the necessary knowledge and skills to effectively recognize and address any suspicious activities related to money laundering or terrorist financing.

9. COMPLIANCE AND ENFORCEMENT

9.1. Our utmost commitment is to fully comply with applicable AML regulations. This entails collaborating with relevant regulatory bodies, courts, law enforcement, and other competent authorities. If you have any inquiries, please don't hesitate to contact our designated Money Laundering Reporting Officer:

Reporting Officer:
Name: Pankaj Mishra
E-mail: complianceofficer@rovi.network

9.2. In our pursuit of ensuring the integrity and transparency of transactions on ROVI Money, we strongly encourage you to report any information you possess or may come across in the future regarding Suspicious Transactions or transactions that appear dubious in nature. Please direct such reports to our Compliance Officer by sending an email to complianceofficer@rovi.network

10. POLICY REVIEW :

10.1. This AML Policy will undergo a review at least once a year to align with regulatory changes, industry practices, and the evolving nature and complexity of our operations. Any updates to this policy will be reflected here. We encourage all stakeholders to regularly revisit this AML Policy and familiarize themselves with any changes. For

previous versions of this AML Policy, please feel free to contact us via email at complianceofficer@rovi.network

10.2. It is important to note that this AML policy serves as a guideline and does not guarantee absolute prevention against money laundering or terrorist financing. We are committed to continually improving our procedures and systems to enhance our ability to prevent such activities.