ANTI MONEY LAUNDERING POLICY

Last updated on 23 June 2023.

Onramp Money is technology solution that allows users to deposit fiat and purchase cryptocurrencies.

OnRamp 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 capitalised 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 operations are aligned with applicable legal requirements and regulations of the jurisdiction we operate in;

1.2. We conduct periodic risk assessments to understand money laundering, terrorist financing and proliferation financing risks associated with our customers and our Platform.

1.3. Appropriate AML procedures are functional and monitored for their effectiveness;

1.4. We shall endeavour to prevent the use of OnRamp Money from facilitating, enabling money laundering or terrorist financing.

1.5. Fully cooperate with law enforcement agencies.

2. USER'S OBLIGATIONS

2.1. By accessing, downloading or using the Platform, users' acknowledge and agree that they shall not use the Platform in any manner that contravenes the Platform's Terms of Service, Privacy Policy, AML Policy or any applicable law. By using, accessing, or downloading this Platform, users agree and consent to any change made by Us without any notice.

2.2. Users acknowledge and agree that any and all information submitted to Us during the use of the Platform is true, accurate and complete. All such rendered information/ Identification Document must belong to the user submitting the information/ Identification Document.

2.3. In case of any change of address, Users must notify and file a fresh proof of address within 6 months of making changes to the address.

2.4. Users shall not engage or conduct any Suspicious Transaction or Money Laundering activity or engage with any person on the Sanctions List. **Sanctions List** means the reference to lists of natural and juridical persons included under any list by any country or government or international authority, including the US Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), the European Union, Monetary Authority or the Monetary Authority of Singapore and relevant applicable laws. "**Suspicious Transaction**" means a transaction, including an attempted transaction, whether or not made in cash, which to a person acting 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. At Our sole discretion, we may block, restrict or terminate access to any user's account if it is found that the user is engaged in or is suspected of engaging in illegal activities.

3. CUSTOMER DUE DILIGENCE

3.1. **KYC:** We understand that our Platform maybe misused by state and non-state actors to facilitate or enable money laundering, terror and proliferation financing. To mitigate those risks and to ensure strict compliance with applicable AML laws. Our identity

verification procedure requires users to provide Us with government issued identity cards or other officially valid documents recognised by competent authorities. All collected information will be processed according to our Privacy Policy available here.

3.2. In view of the above and in accordance with applicable law, we have deployed the following Customer Due Diligence ("**CDD**") in the form of a three-tier Know-Your-Customer ("**KYC**") system:

3.2.1. **Basic KYC:** All users that use the platform must undergo the Basic KYC. At this level, a user must undertake two tasks: One, enter their phone number and enter the OTP send to their phone number by Onramp; Two, submit a government issued valid identity card (Proof of identity). We partner with third-party vendors to verify the details entered by comparing the data inputted by the user with data retrieved from relevant government databases.

3.2.2. **Full KYC:** Based on monthly transactions, users may have to complete a full KYC. At this level, a user must have to complete a Basic KYC, complete a video KYC and submit documents that serve as proof for source of funds.

3.3. KYC is undertaken at the time of onboarding new customers on the Platform and such information will be verified by our compliance team during the course of a user's use of the Platform. To ensure that we continue to hold updated user information or as part of our randomised checks, users may have to undertake any KYC at any point. In such cases, users may be requested to submit additional documents. Such documents include but not limited to a user's form for income tax returns, bank account statement etc. All requested and collected information shall be stored and processed according to our Privacy Policy available here.

3.4. All submitted user identity documents must be in English only. If the identity document is not in English, please submit a translated identity document that is duly notarised by agencies authorised to notarise such documents.

3.5. Please note that the deployed KYC system may differ based on applicable law and jurisdiction. As part of the CDD, we deploy steps to confirm the authenticity of documents submitted by users. We reserve the right to investigate users who are determined to be risky or suspicious. We reserve the right to receive up-to-date documents from users, even if they have passed the identity verification in the past. Such collected information will be processed and stored according to our Privacy Policy available here.

4. ENHANCED DUE DILIGENCE ("EDD"):

4.1. EDD measures are applied to complex, unusually large transactions, unusual patterns of transactions and users categorised as high risk. High-risk customers/users include politically exposed persons ("**PEPs**") or those from high-risk jurisdictions. EDD measures also involve obtaining additional information or verification, increased monitoring and restricting the types or volumes of transactions that can be conducted. Such measures are deployed commensurate with the risk. We carry out the following activities to ensure that the EDD is deployed:

4.1.1. Frequent review of customers' profile/transactions;

4.1.2. Collection of information about the user from available sources;
4.1.3. Conducting independent enquiries on the details provided by the user
4.1.4. Consulting a credible database etc.

4.2. We are prohibited from transacting with individuals, companies and countries that are on the prescribed sanctions list. We will screen against the lists released by the United Nations, Financial Action Task Force, European Union, UK Treasury and US Office of Foreign Assets Control ("**OFAC**") sanctions lists in all jurisdictions in which we operate. In case it is found that a user enables suspicious transactions, then We may file a report with the competent authority. As per applicable rules and regulations, disclosure to such competent authority shall be strictly confidential. For more information on how we collect, process and store information, please consult our Privacy Policy available here.

4.3. In relation to foreign politically exposed persons, in addition to performing CDD measures, we ensure that:
4.3.1. We have appropriate risk-management systems to determine if the customer is politically exposed person;
4.3.2. Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
4.3.3. Take reasonable measures to establish the source of wealth or source of funds;
4.3.4. Conduct enhanced ongoing monitoring of the business relationship.

5. MONITORING TRANSACTIONS

5.1. All customer transactions will be monitored for unusual or suspicious activities.The extent of monitoring shall depend on various factors including upon each User's risk profile. Our Compliance Officer will review and investigate suspicious transactions. In view of applicable law, any suspected, detected or attempted suspicious transaction of proceeds may be reported to the appropriate and competent authority.

5.2. While conducting periodic checks, if we suspect transactions relate to money laundering, terrorist financing or any other illegal activity, then we may seek information to identify and verify the identity of the customer. By accessing, downloading or using the Platform, users acknowledge and agree to assist and fully coorporate with Us in any query, investigation or direction by a competent law enforcement authority.

6. RISK ASSESSMENT

6.1. In line with applicable law, We have adopted a risk-based approach to combating money-laundering and terrorist financing. To mitigate the applicable risks, We categorise our users into high-risk, medium-risk and low-risk. The factors taken into consideration for the risk assessment include but not limited to:
6.1.1. The sufficiency and adequacy of the identification information submitted by the user;
6.1.2. User's geographical location;
6.1.3. Users carrying out extremely complex or high value transactions;
6.1.4. Users carrying out transactions with or within known high-risk jurisdictions;
6.1.5. Countries subject to sanctions, embargos or similar measures;
6.1.6. Countries identified by credible sources to have significant levels of corruption or other criminal activities;

6.1.7. Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.
6.1.8. Financial or social status;
6.1.9. Nature of user's business activity and the regularity or duration of the business relationship;
6.1.10. Guidance notes circulated by various governmental and intergovernmental organisations.

6.2. All information related to the risk profile of a user is kept strictly confidential. The information collected to generate the risk profile is processed and stored according to Privacy Policy. Any disclosure of such confidential information shall be done only in accordance with the Privacy Policy.

6.3. Based on a user's risk profile, at Our sole discretion, We reserve the right to restrict, suspend or terminate any user's operation that contravenes applicable law.

7. RECORD KEEPING

All information collected, processed and stored by Us will be in accordance with our Privacy Policy. Such collected data shall be stored for a period as per applicable law. In case no duration is prescribed under applicable law, We shall retain your information for a duration of 5 years.

8. EMPLOYEE TRAINING AND AWARENESS

All staff undergo regular training to understand AML Policy, recognise suspicious activity to fulfil their AML related responsibilities. Training programmes are updated to reflect changes in regulations or business operations.

9. COMPLIANCE AND ENFORCEMENT

9.1. We are committed to full compliance with applicable AML regulations. This includes cooperation with relevant regulatory bodies, courts, law enforcement and other competent authorities. In case of any queries, please do not hesitate to contact our Money Laundering Reporting Officer:

Name: Nitin Vaid
Address: No 1090C, 3rd Floor, 14th Main, 18th Cross Rd, Sector 3, HSR Layout, Bengaluru, Karnataka 560102
E-mail: complianceofficer@onramp.money

9.2. To improve the integrity and transparency of transactions on OnRamp Money, you are encouraged to report any information you are privy to or become privy to in the future regarding any Suspicious Transactions or transactions you have find or have reason to believe are dubious in nature, to our Compliance Officer by writing to them at complianceofficer@onramp.money.

10. POLICY REVIEW :

10.1. This AML Policy will be reviewed at least once a year in accordance with changes in regulations, industry practices or nature and complexity of our operations. Changes to this policy will be updated here. We urge all stakeholders to revisit this AML Policy and

familiar themselves with any changes. For previous versions of this AML Policy, please do not hesitate to contact us by dropping an e-mail at: complianceofficer@onramp.money

10.2. This AML policy is a guideline and does not guarantee complete prevention against money laundering or terrorist financing. We continue to strive to improve our procedures and systems to prevent such activities.