

Caracol Ltd Anti-Money Laundering (AML) and Know Your Client (KYC) Policy Ver. 3.0 (hereinafter referred to as the «Policy»)

Money laundering is the process of converting Funds derived from illegal activities (fraud, corruption, terrorism, etc.) into other Funds or investments that look legitimate to hide or distort the actual sources of those Funds.

In order to combat the penetration of money derived from criminal activities into the economy and to prevent terrorist activities, countries are engaged in the fight against money laundering. Due to the openness and accessibility of financial markets and the free movement of capital within them, financial institutions may be one way to legalize criminal income.

Therefore, Caracol Ltd is regulated and compliant to the laws and regulations to combat money laundering and terrorist financing:

Banking Act, 1987

Anti-Money Laundering Regulations, 2002

Counter-Terrorism Act, 2002

Recommendations for Money Laundering of FATF

General provisions

This is Policy of Caracol Ltd, a Company incorporated under the laws of the Republic of the Marshall Islands, Reg. No. 114137, with its registered office at Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Marshall Islands, MH 96960 (hereinafter referred to as the «**Company**», «**We**», «**Us**», «**Our**») on combating money laundering, as well as its involvement in identifying and preventing any activity related to money laundering, terrorist financing, and the potential use the Company's products and services for the purpose of money laundering.

The words of which the initial letter is capitalized have meanings defined under the following conditions.

The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions:

Account means Client's registered account on the Company's Platform.

Client means a user who has successfully registered an account on the Platform with the intent to conclude financial transactions.

Company means Caracol Ltd, a Company incorporated under the laws of the Republic of the Marshall Islands, Reg. No. 114137, with its registered office at Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Marshall Islands, MH 96960.

Funds mean money and its equivalents applicable to the authorized activities on the Platform.

Platform means online trading platform available on the Website.

Website / Site referred to stockity.id.

Verification (KYC - Know Your Client)

For verification, We request a document proving the identity of Our Client. It can be:

- a photo of the Client's passport or ID card;
- photos of their bank cards/screenshots of their e-wallets;
- a photo of the Client with the documents specified above in their hand.

In order to comply with the laws on countering money laundering or terrorist financing, the Company may require the Client to submit additional documents such as:

- a utility bill (not older than 3 months);
- a bank reference letter (not older than 3 months);
- a bank statement letter (not older than 3 months);
- documents confirming source of wealth/Funds (for example, salary, sale of property, loan, inheritance);
- the 2nd ID document (for example, driving license);
- notarized copies of the documents specified above.

Documents in languages other than English must be translated into English; the translation must be notarized and sent along with a copy of the original document with a clear photograph.

Clients send the indicated documents to Our compliance team via email: verification@stockity.id in image file formats (Jpg, Jpeg, Pdf). Documents cannot be accepted in rar or zip archives or in doc, docx, or other text formats.

Clients have to provide all documents required within Fourteen (14) calendar days since the Company request.

Verification is carried out within Twenty (20) minutes from the moment the Client provides the full set of documents requested by the Company. In some cases, the Company has the right to extend this period to Seven (7) calendar days.

For additional verification, We duly perform Client verification using the following method - Skype, Zoom conference calls or other types of communication regarding «Face to Face» procedure of verification.

In order for Us to implement the Client verification measures through the KYC and AML procedures set out in this Policy for the uninterrupted, clear and normal conduct of business, We also may engage independent contractors who comply with the high quality standards in verifying Clients as required by applicable law and regulations.

For a more detailed description, refer to Our [Privacy Policy](#).

Requirements for identity documents

Pages of the passport, ID card or other required identification document should be open on both sides (if applicable). The document must be completely visible on the photo / scan, without any edges or corners cut off, and without any glare from the flash or any elements excluded. The personal signature on the document may be covered. All data on the document must be readable and legible. The document will be checked for the use of Photoshop or other image editors. The Client must be of the legal age of majority at the time of account creation. The document must be valid. Watermarking is permitted.

Ways to check the document for validity if there are suspicions it is not valid

AML online check services that are based on the AML Global Watchlist (global AML risk data sources including sanction lists (such as OFAC, UN, HMT, EU, DFAT, and others), law enforcement lists (Interpol, country-specific government and state agencies, and police forces), and international governing regulatory bodies (financial and securities commissions) from around the world.

Requirements for bank cards

Bank card should be completely visible in the photo, without any edges or corners cut off, and without any glare from the flash. The following data should be visible on the photo of the card:

- the cardholder's first and last name;
- the first 6 and the last 4 digits of the card number;
- the card's expiration date.

If the cardholder's name is not listed on the card, then We may request confirmation of the identity the card belongs to. This may be a screenshot of the online bank account where the cardholder's full name is visible. Or it may be a statement from the bank proving that the card was issued to the cardholder. The statement must contain the name of the cardholder, the card number (incomplete data is allowed), the bank operator's signature, and the bank's stamp.

Requirements for electronic wallets (e-wallets)

To verify an e-wallet, a screenshot of a deposit to Caracol Ltd will be required. The screenshot should show the payment itself, the time and date of the transaction, and e-wallet number. Electronic wallets also require a screenshot of the page showing personal data - first and last name, date of birth (if possible). For two screenshots, there should be general information visible to make it clear that the screenshots were taken of the same e-wallet.

Requirements for photos with the documents in hand (selfies)

Passport, ID card or other document must be completely visible on the photo and the data must be readable and legible. The signature may be covered. The Client's face must be completely visible on the photo and match with the photo in the passport (adjusted for age). The passport on the selfie and the passport on the photo / scan should be identical.

Documents in languages other than English must be translated into English; the translation must be notarized and sent along with a copy of the original document with a clear photograph of the Client on it.

Independent contractors who may be engaged by the Company to verify Clients, subject to all necessary regulations and applicable laws regarding the handling of personal data, will accept documents in languages other than English.

Accounts are verified not only to comply with this Policy, but also to ensure the security of the Client's Funds.

Deposits of Funds

The name of the depositor (Client) of Funds should fully comply with the name specified in the registered Account (if the payment system provides the name of the depositor (Client) of Funds) for successful completion of the procedure for crediting Funds. Payments from third parties are prohibited.

The Company has the right to demand strict adherence to the accepted procedure for depositing and withdrawing Funds.

Company Money Laundering Prevention Procedures

It is forbidden to use the Site for the purpose of money laundering. The Company applies advanced anti-money laundering procedures. All transactions are monitored to prevent money laundering, which can have various implications for Clients. The Company reserves the right to refuse to cooperate, terminate cooperation, and cancel transactions of Clients who do not accept or do not comply with these measures to prevent money laundering. Funds accepted by the Company should not be derived from criminal activity. The Company is obliged to report suspicious transactions to the

appropriate authorities. The Company reserves the right to request documents confirming the origin of the Client's Funds.

«Suspicious Transactions». In case of conducting of any transaction entered/withdrawn to and from the Platform that the Company believes is relevant to the possible violation of any law or regulation, or could constitute or be related to terrorist financing, terrorist acts, a terrorist organization, an individual terrorist or to terrorist property, or which is complex or unusual or present an unusual pattern, or has no apparent economic or lawful purpose, or is not the sort of transaction in which any person would normally be expected to engage, Our compliance team will forward the relevant report to the Banking Commissioner of the Republic of the Marshall Islands.

«Suspicious Activities» shall be understood to mean transactions in any instance where there is a suspicion that the person is involved in money laundering or terrorist financing.

Our counter-activities related to «Suspicious Transactions» / «Suspicious Activities»:

- in the event that signs of fraud are detected in the conducting of financial transactions after the crediting of Funds to the Client's Account, We reserve the right to cancel such transactions and block the Client's Account;
- if the Client clearly intends to use their Account for exchange transactions between payment systems, We have the right to decline the Client's request for withdrawal of Funds from their Account;
- in cases where the Company's security service suspects the Client of fraud or deception, We also have the right to block the Client's Account without prior notice and without the possibility of withdrawing Funds.

The mitigation of such risks is accompanied by reports to the Banking Commissioner of the Republic of the Marshall Islands as soon as practicable, if the Compliance team reporting on AML/CFT knows, suspects or has reasonable grounds to know or suspect that such Client is engaged in money laundering or terrorist financing, and if there is reason to suspect a transaction whose purpose is money laundering or terrorist financing according to Anti-Money Laundering Regulations, 2002.

Money laundering prevention procedures may have the following consequences for Clients and impose on them the following duties:

1. Clients must provide all the requested personal data when opening an Account. This includes a full and correct name; copy of the first two pages of passport or a copy

of valid ID showing the following details: i. number and country of issuance; ii. issue and expiry date; iii. signature of the person (if any); permanent address; contact email address; and written authority to obtain independent verification of any information provided. Any other names previously held; telephone (not including mobile phone number); date and place of birth; nationalities and citizenships held currently and previously; occupation and name of employer (if self-employed, the nature of the self-employment); signature; purpose of the account and the potential account activity; and source of income or wealth may be requested additionally.

2. Withdrawals can only be made in the name of the Account holder. If the Client deposits Funds into their Account using a bank transfer, the Funds can only be transferred to the owner of the bank account. The Client undertakes to provide the correct account number and correctly provide their name for all money transfers to the Company. If the Client credits their Account using a credit/debit card, the Funds will be transferred only to that same card.

3. Clients must register Accounts for themselves only.

4. Clients cannot accept Funds from one or more third persons in order to manage Funds on their behalf of or in interest via their Accounts.

5. It is prohibited to sell, transfer and/or purchase Accounts to or from other Clients or third parties. The transfer of Funds between Clients within the Platform, is also prohibited.

6. The Client is allowed to have only one Account. Withdrawals or compensation cannot be transferred to the Accounts opened using fictitious names, or to multiple Accounts opened by the same Client.

7. At its own discretion or in accordance with the provisions on conducting Client identification procedures, the Company may request from the Client an identity document (for example, a certified copy of their passport or another document that the Company deems necessary under certain circumstances). The Company may also temporarily block the Account until complete information (proof of the identity and address of the Client, the source of their Funds and/or the source of their income). The Client has to provide such a document and information required within Fourteen (14) calendar days since the Company request. The Company reviews the submitted documents and information within Thirty (30) calendar days.

8. The Client agrees that We may use their personal data provided for the appropriate anti-fraud checks. The personal data that the Client provides may be transferred to the appropriate organizations or agencies that may require such

information in order to combat fraud.

9. We record telephone conversations and electronic correspondence of the Clients with Our support team, regarding operations on the Platform as well as the Client's activity on the Platform. Records can also be used for quality control purposes and fraud prevention.

10. The Company has the right to conduct at least one (1) additional Client identification procedure with the provision of documents in accordance with Our Know Your Client (KYC) Policy. This identification will aim at reducing the risk of fraud with personal data.

11. The Company has the right to conduct the Client identification procedure with the provision of documents in accordance with Our Know Your Client (KYC) Policy at least once per five (5) years.

12. In the event that the Client's identifiable information changes (e.g., due to expiry, etc.), the Company shall carry out a new verification procedure on the basis of the Company Know Your Client (KYC) Policy.

13. We have the right and duty not to accept information provided by the Client if We know or have reason to believe that this information is untrue, inaccurate, or incomplete. In this case, We may contact the Client for clarification or correction of this information.

14. The Company declares that, in order to comply with this AML Policy, transfers of Funds by the Clients are permitted solely for the purpose of carrying out trading operations on the Platform. If the Company reasonably believes that transfers of Funds are being used by the Client in violation of laws and/or Our AML Policy, and/or for the purposes other than the Company's services offered, the Company reserves the right to block the Client's Account to prevent such a violation.

If you have any additional questions, please contact Us by email: verification@stockity.id.

Caracol Ltd

Address: Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Marshall Islands, MH96960