



TRUSTDICE ANTI MONEY LAUNDERING ("AML") AND KNOW YOUR CUSTOMER ("KYC") POLICY

Introduction

TrustDice has put in place an Anti-Money Laundering / Counter-Terrorist Financing Policy and a Know Your Customer Policy (collectively, the “AML Policies”). The Policies are revisited periodically and amended from time to time based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity including money laundering and terrorist financing. All senior management and employees of TrustDice are required to acknowledge and be familiar with the Policies.

This document covers AML Policies regarding TrustDice’s gaming services, which is TrustDice’s main business activity.

Money Laundering Risks

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Terrorist financing is an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes.

The risk of money laundering or terrorist financing on TrustDice is extremely low.

TrustDice does not engage in any exchange transactions between currencies, whether in crypto or fiat. Clients can only deposit cryptocurrency (BTC) and withdraw the same cryptocurrency (BTC), with no exchange activity happening in between. TrustDice uses third party crypto transaction monitoring and source of funds software to track and tag funds deposited into its platform, making it extremely unattractive for potential bad actors attempting to move illicit funds.

All Client funds remain in “virtual” currencies and are never converted to any other currencies. TrustDice requires KYC identification documents from Clients that have deposited more than \$100 worth of currencies as an extra measure of risk reduction and compliance.

AML/KYC Policies Framework

The Policies are designed to lay down a framework to:

- prevent TrustDice from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities;
- enable TrustDice to know and understand its customers, clientele, contributors, and other contacts with which TrustDice has any financial dealings with (collectively, “Clients”) and their financial background and source of funds better, which in turn would help it to manage its risks prudently;
- put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws, procedures and regulatory guidelines; and
- equip employees and contractors of TrustDice with the necessary training and measures to deal with matters concerning KYC/AML procedures and reporting obligations.

Our Policies will be reviewed and updated on a regular basis to ensure appropriate procedures and internal controls are in place to account for both changes in regulations and changes in our business.

Risk-Based Approach

TrustDice adopts and maintains a Risk-Based Approach (“RBA”) towards assessing and containing the money laundering and terrorist financing risks arising from any transactions it has with Clients. The guidelines are as follows:

- Before entering into any transaction or proposed transaction, necessary checks shall be conducted in line with the RBA so as to ensure that the identity of the Clients does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations;
- For the purpose of risk categorization of the Clients, the relevant information shall be obtained from the Clients at or before the time of entering into a transaction;

- The risk categorization process for different types of Clients may take into account the background of the Clients, country of origin, sources of funds, volume of turnover or deposits, as well as social and financial background;
- The outcome of the risk categorization process shall be decided based on the relevant information provided by the Clients at the time of commencement of business relationship;
- Enhanced due diligence would be required for higher-risk Clients, especially those for whom the sources of funds are not clear, or for transactions of higher value and frequency, which shall be determined by TrustDice at its sole and absolute discretion; and
- TrustDice must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the TrustDice in compliance with the relevant legislations in place.

Customer Identification

The Customer Identification Program is to be carried out:

- If Clients have deposited more than \$100 worth of currencies; and
- when there is any doubt about the authenticity, veracity, or adequacy of the previously obtained Clients 'identification data.

TrustDice:

- requires Clients to provide proof of identification and proof of residence; and
- does not under any circumstances permit any transaction to be made with incomplete identity and residence verification information.

When there shall be any suspicion of money laundering or terrorism financing activities, or where there shall be any doubt about the adequacy or veracity of previously obtained Clients 'identification data, the due diligence measures shall be reviewed,

including verifying the identity of the Client again and obtaining information regarding the purpose and intended nature of the relationship with TrustDice.

TrustDice does not serve clients from certain regions that are deemed high-risk or unwelcoming from a legal or regulatory perspective, including Cuba, Iran, North Korea, Syria, and the United States of America.

Sanctions

TrustDice does not open accounts or transact with individuals that are on prescribed sanctions lists. TrustDice screens against United Nations, European Union, UK Treasury, US Office of Foreign Assets Control (OFAC), and other sanctions lists in all jurisdictions in which TrustDice operates.

Politically Exposed Persons

TrustDice does not open accounts or transact with individuals who are Politically Exposed Persons (PEPs), or their family members. TrustDice screens all Clients against global PEP lists before they are allowed to establish a relationship with TrustDice.

Required Information

TrustDice accepts only natural persons as Clients, not legal entities. Once they have deposited more than \$100 worth of currencies, Clients go through an automated verification process where they submit:

- Full name;
- Date of birth;
- A unique photo of them holding their government-issued photo ID.

All submitted client information is manually reviewed. For clients who cannot be verified through automated means (geolocation, algorithmic face detection, sanctions list check), enhanced due diligence is requested as described below.

Government-issued ID

Verification of identity is required by obtaining a high-resolution, non-expired copy of the Client's government-issued ID (passport, national identity card, or a driver's license). The submitted imaged requirements include:

- Full color image. Black and white, watermarked, etc. are not accepted;
- Legible. All information on the ID must be completely clear and readable. TrustDice does not accept IDs that are torn or worn out; and
- Background. The edges of the ID document must be clearly visible on a contrasting background.

Proof of residence

Verification of residence is required by obtaining a copy of an acceptable address proof document issued in the 3 months prior to Customer Identification. The document must carry the Client's name and address.

A valid proof of residence document can be:

- bank statement;
- debit or credit card statement;
- utility bill (water, electricity, gas, internet, phone);
- payroll statement or official salary document from employer; • insurance statement;
- tax document; or
- residence certificate.

Proof of residence documents must contain the Client's name, address, and be dated less than 3 months ago.

Unique photo of Client

Further verification is requested from Clients by submitting a unique photo of themselves holding their government-issued ID as well as a unique handwritten note. In the photo, the Client must be visibly smiling. This allows TrustDice to easily prove that the Client's picture was not stolen or photoshopped, and is being used exclusively for TrustDice.

The ID the Client holds in their hand:

- must be the same government-issued ID the Client submitted previously; and
- must be fully clear and readable.

The note the Client holds in their hand:

- must be handwritten (not typed);
- must be in English;
- must contain today's date;
- must contain the sentence: For playing at trustdice.win only; and
- must contain the Client's signature.

Verification

Based on the risk, and to the extent reasonable and practicable, we ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about Clients. Our AML Compliance Officer analyzes the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer.

We may decide to use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source;

- Checking references with other financial institutions;
- Analyzing whether there is logical consistency between the identifying information provided, such as the Clients 'name, street address, postal code, and date of birth;
- Utilizing complex device identification (such as “digital fingerprints” or IP geo-location checks); and
- Obtaining a notarized or certified true copy of an individual’s birth certificate or government-issued ID for valid identification.

Internal controls

TrustDice implements and maintains internal controls for the purpose of ensuring that all of its operations comply with AML legal requirements and that all required reports are made on a timely basis.

Compliance Officer

The Compliance Officer is the person, duly authorized by TrustDice, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer’s responsibility to supervise all aspects of TrustDice’s anti-money laundering and counter-terrorist financing, including but not limited to:

- Collecting Clients 'identification information;
- Establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations;
- Monitoring transactions and investigating any significant deviations from normal activity;
- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs;

- Updating risk assessment regularly;
- Providing law enforcement with information as required under the applicable laws and regulations.
- The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing, and other illegal activity.

Monitoring and Reporting

TrustDice diligently monitors transactions for suspicious activity. Transactions that are unusual are carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose. When such suspicious activity is detected, the Compliance Officer will determine whether a filing with any law enforcement authority is necessary.

Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and TrustDice may wish to make a filing with a law enforcement authority, even if no money is lost as a result of the transaction.

The Compliance Officer initially makes the decision of whether a transaction is potentially suspicious. Once the Compliance Officer has finished his review of the transaction details, he makes the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be made.

For the purpose of the Policies, a “Suspicious Transaction” means a transaction or attempted transaction, which to a person acting in good faith,

- gives rise to a reasonable ground of suspicion that it may involve proceeds of criminal or other illicit activity, regardless of the value involved;
- appears to be made in circumstances of unusual or unjustified complexity;
- appears to have no economic rationale or bona fide purpose; and

- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Ongoing monitoring is an essential element of effective implementation. TrustDice diligently monitors transactions for Suspicious Transactions and other suspicious activity.

Record-keeping

Our AML Compliance Officer is responsible for ensuring that AML records are maintained properly.

We document our verification, including all identifying information provided by a Client, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We keep records containing a description of any document that we relied on to verify a Client's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we retain documents that describe the methods and the results of any measures we took to verify the identity of a Client.

We also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We retain records of all identification information for seven years after the account has been closed, or as long as reasonably necessary to comply with applicable regulations; we retain records made about verification of the customer's identity for seven years after the record is made, or as long as reasonably necessary to comply with applicable regulations.

Training

All new employees receive anti-money laundering training as part of the mandatory new-hire training program. All applicable employees are also required to complete AML and KYC training annually. Participation in additional targeted training programs is required for all employees with day-to-day AML and KYC responsibilities.

Our training includes, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags (3) what employees' roles are in TrustDice's compliance efforts and how to perform them; (4) TrustDice's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance.

Our operations are regularly reviewed to check whether certain employees require specialized additional training. Written procedures are updated to reflect any such changes.