

KYC, AML, CFT & CRIMINAL ACTIVITY POLICY

Introduction

GT Holding B.V., having its registered address at Schottegatweg Oost 10, Unit 1 – 9 Bon Bini Business Center Curaçao, licensed to conduct online gaming operations by the Government of Curaçao under Reg No.HE 422126, organizes gambling via the tether.bet website. Under the license conditions issued by Curaçao, GT Holding B.V. is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity.

The objective of the policy

GT Holding B.V. is fully committed to be constantly vigilant to prevent money laundering and combat the financing of terrorism in order to minimize and manage risks such as the risks to its reputational risk, legal risk and regulatory risk. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused in furtherance of these crimes. GT Holding B.V. will endeavour to keep itself updated with developments both at the national and international level on any initiatives to prevent money laundering and the financing of terrorism. It commits itself to protect, at all times, the organization and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorists and other criminal activities.

Obligations

In order to adhere to the requirements of the license conditions, the regulations and any guidance notes GT Holding B.V. shall put in place the following procedures:

Customer Verification

Every customer is subject to completing the Know Your Customer (KYC) process. As part of the registration process, all customers are expected to provide a range of personal details, including several mandatory fields that must be filed prior to registration being able to be completed by the customer. Sanctions, PEP, financial crime and adverse media screening of customers against relevant watchlists will be conducted upon the registration of a player with the platform deemed necessary.

This check will ensure that these three main points are addressed:

- The customer's identity is genuine
- The customer is at least 18 years old

- The customer's payment details are genuine

Any customers that fail this check as per items 1 and 2 above will be expected to undergo a manual KYC process. This would result in the customer requiring to provide images of their identity, proof of age and proof of address.

In the event that a customer provides copies of identification data (such as an identity card) in order to complete the customer verification process, the data is encrypted and stored securely on servers located in the Data Centre in Sweden. This information can only be accessed by members of the Fraud team. No other departmental staff are able to gain access to this drive.

For this purpose, the process for the registration of Players provided under the General Terms and Conditions provides for the due diligence process that must be carried out before the opening of a User Account.

- keep at all times a secure online list of all registered Players.
- retain identification and transactional documentation as defined in the law regulations and guidance notes.
- provide initial and ongoing training to all relevant staff so that they are aware of their personal responsibilities and the procedures in respect of identifying Players, monitoring Player activity, record-keeping and reporting any unusual/suspicious transactions.
- ensure that this policy is developed and maintained in line with evolving statutory and regulatory obligations and advice from the relevant authorities.
- examine with special attention, and to the extent possible, the background and purpose of any complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.
- cooperate with all relevant administrative, enforcement and judicial authorities in their endeavour to prevent and detect criminal activity.

Anti-Money Laundering Procedures

Where any additional risk is subsequently discovered, customers will also undergo an Enhanced Due Diligence process, where the account will be blocked and an additional round of ID verification will take place – this will be in the form of images of their identity, proof of age, proof of address and the front side of the bank card used to deposit (if applicable).

If there are any doubts about the actions of a verified customer, the account will be blocked and the customer will be requested to provide us with an additional round of ID documentation. This will also be escalated to the Money Laundering Reporting Officer (MLRO) if there are suspicions of Money Laundering.

All staff are trained on Money Laundering awareness and reporting processes upon induction by the Compliance Officer and other line managers and receive ongoing training where appropriate. A companywide refresher training module and test are also carried out annually. The Payments

and Fraud departments actively screen bank cards and e-wallet transactions (especially those from new customers) in order to identify any potential high risks. They do this both through manual searches of all the deposits coming in and also with the assistance of selected triggers within an automated User Alert program of the Internal Gaming System (IGS). All withdrawal requests for verified customers over £300 are manually reviewed by the Payments & Fraud team prior to processing, whilst in situations where there are suspicions around accounts that have already been verified, there also is a feature in the system where staff can prevent a customer from making automatic withdrawals. In these situations, all withdrawal requests are reviewed manually by the Payments and Fraud teams prior to authorization.

Staff will also view the velocity of transactions by customer's payment method on a daily basis to ensure that they are using the website for genuine betting purposes. Customers are only ever able to transact with GT Holding B.V. and not any third parties.

Customers should only be using a payment method that is in their own name. Any account holder found to be using a payment method in the name of another individual will be blocked immediately and Enhanced Due Diligence will be conducted on both the customer and owner of the payment method. Once both parties are fully verified, the entire balance will be returned to the initial payment method used to deposit. The customer will then be expected to register their own payment method to use on their account.

Fraud Prevention

There are various triggers in place in the Payments, Fraud, Customer Service and Trading teams that may identify customers conducting fraud. Numerous actions can take place thereafter, including the limitation on the markets and stakes, and a manual review of all withdrawal orders prior to processing.

Reporting Responsibilities

GT Holding B.V. is fully aware of its responsibilities in relation to international legislation around handling customers who are suspected of using the business to transact with the proceeds of crime and will endeavour to ensure that existing AML procedures are adhered to in all circumstances.

Any suspicious transaction report will be sent to the customer's country authorities as soon as it's been completed by GT Holding B.V., and also retained on record internally.

GT Holding B.V. has one senior member of staff that handles any escalated suspicious activity in relation to possible Money Laundering. This is the Money Laundering Reporting Officer (MLRO). In turn, when it is confirmed by MLRO that suspicious activity has taken place, it is his/her responsibility to report this to the authorities.

Terrorist Financing & High-Risk Customers

Existing customer relationships are monitored on an ongoing basis. The High-Risk Customer Database, which contains lists of customers from the most High-Risk jurisdictions and suspicious accounts is reviewed and updated on an ongoing basis. All possible Politically Exposed Persons are reviewed on a quarterly basis or if they hit various high-risk thresholds, whilst the User Alert program of the back office will also flag customers who have deposited either €2,000 within 24 hours or €10,000 within 90 days.

Other customers that may be classified as high-risk are those that are from jurisdictions identified as sensitive regions by the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). In such cases, Enhanced Due Diligence will always be conducted on new registrations from the High-Risk Country List.

Routine screenings are conducted against the following lists to ensure that no high-risk individuals associated with Terrorist Financing register with GT Holding B.V.: • The full list of financial sanctions targets on the HM Treasury website (United Kingdom) • The UN Sanctions Committee List

In addition, ad hoc sanctions notifications will be provided by the Guernsey Financial Intelligence Service (GFIS) – any named individuals listed will be reviewed on the spot and again on an ongoing basis to ensure that they are not a GT Holding B.V. customer.

An explicit client admission policy must include a description of the clients that could entail a degree of risk above the average, according to the factors determined by the obliged person in accordance with the applicable international standards. This policy must be gradual, and precautions shall be adopted in relation to those clients that present a risk level above the average.

The categories of 'risk clients' must be specified in the handbook, to which must be added a suitable description of the alert systems which permit to detect and carry out a special follow-up of these clients.

Moreover, tether.bet shall:

- not accept opening anonymous Accounts or Accounts with fictitious names such where the true beneficial owner is not known.
- not accept cash from Players. Funds may be received from Players only by any of the following methods: credit cards, debit cards, electronic transfer, wire transfer cheques and any other method.
- not register a Player who is under eighteen (18) years of age.
- only register a single account in the name of a particular person: multi-account practices are strictly prohibited.
- transfer payments of winnings or refunds back to the same route from where the funds

originated, where possible.

- not accept a wager unless a User Account has been established in the name of the Player and there are adequate funds in the Account to cover the amount of the wager.
- not accept a wager unless the funds necessary to cover the amount of the wager are provided in an approved way.

- verify the source of wealth and source of funds on a risk-sensitive basis.
- not accept Players residing or playing from non-reputable jurisdictions.
- not make a payment in excess of two thousand Euro (€2000) out of a User Account to a Player until the Player's identity, age, place of residence, and source of wealth have been verified.

- if it becomes aware that a person has provided false information when providing due diligence documents, not register such a person. Where that person has already been registered, tether.bet shall immediately cancel that person's registration as a Player with the company.

Effective from: 01.02.2024.

Last updated: 25.03.2026.