

Anti-Money Laundering and Counter-Terrorism Financing (AML) Policy

Approving Official:	Aftermath BV Board
Responsible Office:	Compliance Officer
Effective Date:	25 May 2025 [pending licence approval]
Next Review Date:	30 April 2026

1. Policy Statement

- 1.1 It is SBX's intention to comply with relevant laws and regulations that apply to it in relation to anti-money laundering, combating financing of terrorism and financing of proliferation.
- 1.2 We strictly prohibit the use of our Services for any illicit objective or activities, including ML, TF, FP and sanctions violations. We understand the harm that can be caused by money laundering, terrorist financing and the proliferation of weapons of mass destruction purposes, and are committed to safeguarding against this including by:
 - (a) undertaking and regularly updating an ML and TF risk assessment for our business that underpins the design of the AML Program. This involves identifying and assessing ML, TF or FP risk that may occur within our business, at a business-wide level and category level, as risks relating to customer or transaction, product, payment methods and geographic location. Understanding and ongoing assessment of these risks allows us to apply a risk-based approach to combat ML, TF and FP;
 - (b) designing and implementing our AML Program, written policies, procedures, and controls using this risk-based approach, comprising a range of measures designed to manage and mitigate the risk of ML, TF and FP, that protects our organization against ML/TF (commensurate with the identified risk) and is compliant with legal and regulatory requirements;

- (c) appointing a senior manager to oversee the implementation of our AML Program and related policies, procedures, and controls;
 - (d) providing our personnel with adequate and ongoing education and training;
 - (e) arranging and responding to independent reviews, and conducting ongoing monitoring and internal audits of our AML Program, policy, procedures, and controls to ensure effectiveness;
 - (f) working co-operatively with the CGA and other relevant bodies;
 - (g) continuously improving this Policy and the AML Program with regular reviews including to take account of changes to law, best practice or guidance and internal or external audits;
 - (h) documenting the actions and reviews mentioned above.
- 1.3 We take this approach to ensure legal and regulatory compliance, as part of commercial risk management processes, and as part of our commitment to help preserve a high standard of integrity and reputation of the industry, the stability and integrity of the financial system and the protection of society from crime.
- 1.4 The objective of this AML Policy is to outline the main procedures that we have established to detect and mitigate the risk of ML, TF and FP in relation to our business, that are more fully explained and implemented throughout our AML Program and related processes and procedures.

2. Purpose

- 2.1 The Site is owned and operated by Aftermath BV ("**SBX**", "**we**" or "**us**"), a company registered in Curacao. SBX operates an online casino and sports betting platform at the Site, and is licensed and regulated by an online gambling license issued by the CGA.
- 2.2 This Policy outlines our approach and procedures for mitigating and countering Money Laundering (ML), Terrorist Financing (TF) and financing of proliferation (FP). We have developed this Policy having regard and in adherence to the National Ordinance on Identification when rendering Services (NOIS), the National Ordinance on the Reporting Unusual Transactions (NORUT), the Sanction National

Ordinance, the Kingdom Sanction Act and the Regulations, and as supplemented by best practice guidelines issued for the gaming industry. We acknowledge that violation of these laws and the Regulations may subject us to administrative and criminal sanctions.

- 2.3 We recognize that our Services could be exploited by individuals or groups to use or launder criminal proceeds or facilitate terrorist financing. We have assessed these risks and are dedicated to cultivating a culture of compliance within the organization, emphasizing the importance of identifying, assessing and mitigating the risk of ML, TF and FP.

3. Audience

This Policy applies to all of our employees and contractors, and to all contractors and service providers to SBX who are involved in anti ML/TF/FP functions, or activities carried out for or on behalf of SBX in the course of its business.

4. Definitions

AML Program means Aftermath BV's anti-money laundering compliance program.

CGA means Curacao Gaming Authority.

Financing of Proliferation or **FP** is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

Financing of Terrorism or **TF** is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population or compel a government or an international organization to do or not do something. In TF, the funds do not need to have been derived from illegal origin (as is the case with ML).

Money Laundering or **ML** covers all acts done with money or property of illegal origin to change its identity, so that it appears to have originated from a legitimate source. There are three typical stages in the ML process:

- **Placement:** Illegal proceeds are introduced to the financial system, where the proceeds generated from criminal activities is converted into a monetary instrument. In an online casino context, this could be by funding casino accounts.
- **Layering:** Converting the proceeds of crime into another form to hide the audit trail, source and ownership of funds. In an online casino context, this could include transfers from one account to another (with the same operator or different operators)
- **Integration:** Recovering the funds in a way that looks legitimate, such as for normal business or personal transaction use. In an online casino context, this could include withdrawing funds to purchase assets

PEP or Politically Exposed Person means persons who are or have been entrusted with a prominent function by a domestic or foreign entity or international organisation, such as Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials, and direct family members and close associates.

Policy means this Anti-Money Laundering and Counter-Terrorism Financing (AML) Policy.

Regulations means the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction applicable to Curacao casinos and providers of online games.

Services means our products and services provided in connection with the Site.

Site means sbx.com.

5. Policy Implementation

5.1 Personnel and training

- 5.1.1 We have a senior manager (Compliance Officer) who is responsible for implementing, managing and overseeing our AML measures and monitoring compliance with relevant laws and our AML Program, including this Policy. These responsibilities include:

- ensuring compliance with Curacao laws and regulations regarding AML;
- reviewing and investigating any unusual activities reported, determining whether external reporting is required, preparing suspicious matter reports and keeping all records
- facilitating staff training sessions on compliance issues;
- updating AML documentation;
- assessing new or varied regulatory requirements or changes to the business;
- identifying and providing recommendations on situations of higher risk;
- reporting to our Board and others in senior management on AML matters;
- staying informed about local and international developments related to ML and TF and suggesting and testing improvements.

5.1.2 All of our employees, directors, and officers, regardless of their position, must comply with this Policy and remain vigilant in preventing ML, TF and FP. If any of our personnel suspect or believe that any transaction or potential transaction or other behaviour may involve criminal conduct, they must report this to a relevant manager immediately.

5.1.3 We will ensure that all of our employees receive appropriate training for their position, including to be able to assist with customer due diligence, and identify and report unusual activities. All staff will receive regular refresher training on ML, TF and FP obligations and risks at least once every year.

5.1.4 We will also follow high standards in the recruitment of our staff including background checks and selection of service providers, as part of our commitment to minimizing ML, TF and FP risk.

5.2 Business Risk Assessment

5.2.1 SBX has conducted an enterprise wide risk assessment of its business which has been relied on to establish its AML Program. The overall risk assessment looks at the ways in which our business could be used to engage in ML, TF or FP activities, and the likelihood and consequences of those risks occurring. Risks are further categorised into environmental, customer, business, channel/delivery, product/service and jurisdiction risk. This is captured in our ML/TF Risk Assessment.

5.2.2 The business risk assessment will be reviewed and updated in accordance with our Risk Assessment Methodology, which includes whenever there are material

changes to AML laws or regulations, or changes to our business (such as new payment methods or markets) and at least once a year.

5.3 Customer Risk Assessment

5.3.1 All SBX customers will be risk rated from an ML/TF perspective. The risk ratings are low, medium and high. Customers will be low risk upon creating an account with SBX unless initial screening results (such as PEP or sanctions) indicate a higher risk. There are various inputs that will inform and potentially change this risk rating during the course of the relationship.

5.3.2 For example, a customer's risk rating will be reviewed upon the following events:

- (a) appearing on a transaction monitoring report or alert, including in sanctions and PEP screening (as per the Transaction Monitoring Process);
- (b) identification of any ML/TF red flags that have been reported (for example, such as under the Law Enforcement and Third Party Requests Process);
- (c) upon enhanced customer due diligence being conducted (as per the Customer Due Diligence Process);
- (d) being subject of an unusual matter or suspicious matter report (as per the UAR and SMR Process);
- (e) where they are a high risk or medium risk customer, on a regular basis (as per the AML Program).

5.3.3 The ML/TF Risk Assessment includes consideration of countries (other than Restricted Jurisdictions) that are high, medium or low risk.

5.4 Customer Acceptance Policy

5.4.1 The following types of customers present a higher or unacceptable level of risk and are not permitted customers:

- (a) minors (as per the KYC Review Process);
- (b) beneficial owners (disclosed or undisclosed) or agents of customers (persons or entities that are not the customer);
- (c) any customer type other than an individual, such as a company or trust;

- (d) sanctioned persons (as per the PEP and Sanctions Process); and
- (e) those in a Restricted Jurisdiction (as per the Restricted Jurisdictions Process).

5.4.2 Where technically practicable, we will not onboard, or will otherwise block or suspend customers who we become aware:

- (a) fail to provide requested identification information or do not pass identity verification as we require (unless there is a valid reason for the delay);
- (b) provide fake, fraudulent or tampered identification documents;
- (c) conceal or attempt to conceal their true location or identity;
- (d) are from or located in a Restricted Jurisdiction;
- (e) are subject to U.S., EU, or other relevant sanctions lists under our PEP and Sanctions Process;
- (f) are subject to a self-exclusion.

5.4.3 Additionally, we reserve the right to block or suspend Users at our sole discretion as outlined in our Terms of Service.

5.4.4 Under our PEP and Sanctions Process, any identified PEP or close associate or family member will be reviewed by senior management and if permitted to hold or maintain an account will be noted as high risk and subject to enhanced due diligence (depending on the category of PEP) which may include determining source of wealth.

5.4.5 Customer Due Diligence may be undertaken on a customer in response to various triggers or events, and may also adjust the customer's risk rating.

5.5 Customer Due Diligence

5.5.1 SBX has adopted a risk-based Customer Due Diligence (CDD) process to develop a risk profile for customers and take appropriate action depending on the level of risk. These processes include collecting specific information on a customer, verifying that information where relevant triggers occur, having systems in place to detect

third party activity on an account, screening a customer against relevant databases and ongoing monitoring of customer activity.

5.5.2 By following a risk-based approach, the appropriate level of due diligence can be applied to customers (the higher the ML/FT risk is, the greater the level of due diligence will be applied).

5.5.3 SBX acknowledges a key mitigant in relation to ML, TF and FP risk is being able to confirm a customer's identity. We have implemented proportionate and targeted controls, policies, and procedures in this area and apply appropriate Know-Your-Customer (KYC) measures to our customer base, including as set out below.

- (a) **Collecting Customer Information:** We collect details from each customer who registers with the Site and at other times when they use our Services, so that we can form a reasonable belief about their identity. Information collected initially as part of the registration process will include name, address, email address, date of birth (collectively, "**KYC Information**"). Customers are required to keep their KYC Information accurate and up to date under our Terms of Service.
- (b) **Verifying Customer Information:** When a customer deposits a certain amount or more of their own money (currently equivalent of XCG5,000); or seeks to withdraw a certain amount or more, and on other occasions where appropriate, we will verify the customer's identity based on services from third-party providers, or information we hold, or a combination of both. This may include us or our third party providers checking a customer's KYC Information against a valid (unexpired) passport, driving licence or national ID document or other reliable, independent source. It may also include collecting additional information such as place of birth, nationality and ID number. Any pending withdrawals may be held until KYC Information is verified or updated as requested by us.
- (c) **Excluding and Geoblocking Restricted Jurisdictions:** Our Terms of Service confirm that we do not accept customers from any Restricted Jurisdiction, which include jurisdictions that present a high ML and/or TF risk or are subject to U.S., EU, or other global sanctions. Each User warrants under the Terms of Service that they are not using the Site or Services from the Restricted Jurisdiction. We use IP address-based geo-blocking to prevent access from Restricted Jurisdictions. As part of the

onboarding process, customers must provide their physical address to confirm that they are not in a Restricted Jurisdiction (attempting to use a Restricted Jurisdiction will block registration).

- 5.5.4 Upon creation of an account it is considered that the purpose of and intended nature of the relationship is for the customer to engage in wagering activity for recreational purposes, unless circumstances arise that indicate otherwise. Where there is unusual activity inconsistent with that nature/purpose, further due diligence will be undertaken which may include enquiries as to customer's source of wealth and expected level of activity.
- 5.5.5 When a relevant ML/TF red flag is triggered and a customer is categorized as potentially high risk, the relevant customer's account will be subject to Enhanced Due Diligence (EDD). Red flags are raised via regular reporting that looks for ML/TF triggers and typologies and may also arise from interactions with the customer or reports from our third party providers or government or regulatory agencies.
- 5.5.6 EDD may involve requiring the customer to provide documents evidencing, or re-confirming, the customer's KYC Information and source of funds and wealth. Documentation or further information requested may include:
 - (a) identification number (passport number, taxpayer identification number, alien identification card number, or another government-issued document with a photograph);
 - (b) valid government-issued identification document (e.g., passport);
 - (c) utility bill less than 6 months old;
 - (d) occupation and previous addresses;
 - (e) source of funds and wealth (eg tax returns, payslips, bank/account statements) and customer's expected level of activity.
- 5.5.7 SBX may use third-party service providers to verify this information and/or such documents may be reviewed by our personnel for authenticity.
- 5.5.8 A customer may be considered high risk if, for example, we have doubts regarding the KYC Information provided, or the customer's behaviour is not in line with their usual profile, or they are categorized as a Politically Exposed Person or appear on other screening results. A high risk customer will be subject to ongoing monitoring,

until such time as they are no longer categorized as high risk or the account is closed.

- 5.5.9 Customers that are categorised as low or medium risk are also subject to internal monitoring and we may request EDD type of information from customers that are not categorized as high risk but that demonstrate ML/TF red flags.

5.6 Ongoing Monitoring

- 5.6.1 We will continuously monitor our customers' activity to help detect any behavior or circumstances indicating ML, TF, FP, sanctions breaches, or other illicit activities, and to ensure customers' behaviour is consistent with our knowledge of the customer, their business and risk. This involves the following:

- (a) **Changes to ID details:** SBX will monitor and seek to verify any requested changes to a customer's KYC details and require KYC refresh as particular intervals (depending on customer risk rating).
- (b) **Transaction Monitoring for Restricted Jurisdictions:** We do not allow customers to open or operate accounts from Restricted Jurisdictions when information we hold suggests the customer or their funds are from such jurisdictions.
- (c) **Transaction Monitoring for Sanctioned Parties and PEPs:** We periodically re-screen our customers against sanctions databases and the Politically Exposed Persons database.
- (d) **Identification of Unusual Activity:** We monitor a customer's account activity for unusual size, volume, patterns, or types of transactions, considering ML and TF risk factors and red flags. Regular reports on unusual, complex, high-risk, or suspicious customer activity are generated and reviewed by staff and can be escalated to senior management to determine appropriate action to take, which may include determining the source of funds. When such behaviour is identified, we may refuse withdrawal attempts while we investigate, and/or request additional information from the customer.
- (e) **Anti-Mixing Measures:** We prohibit the use of anonymity-enhancing technologies such as mixers, tumblers, or certain coins and tokens in connection with the Site. If we detect the use of such technologies on our

Site, we will disallow them and address suspicious deposit or withdrawal patterns on a case-by-case basis taking any action as required by our policies.

- (f) **Third Party Review:** We will use an experienced third party in financial crime to assist in reviewing crypto deposits and withdrawals for signs of fraud or suspicious behavior. Accounts flagged for potential illicit behavior are suspended while they are reviewed. As a result of flagging and subsequent investigation, we may request proof of wealth from customer and refuse withdrawals to high-risk addresses.
- (g) **Withdrawal Threshold KYC:** The ability for a customer to withdraw from their account may be suspended until adequate due diligence is completed. This measure is applied based on withdrawal thresholds, determined by the risk characterization associated with the account and/or customer.
- (h) **Ban Evasion Detection:** As per our Terms of Service, each customer is only allowed one account on the Site. We use database matching criteria to help detect and block the use of multiple accounts by a single customer and use of an account by third parties other than the customer.
- (i) **Time Zone Monitoring:** Where possible we collect and check our customer device location information against Restricted Jurisdictions to detect if they are using software to mask their true location and investigate or suspend the account if this appears to be the case.
- (j) **Vendor Management:** We periodically assess the performance of key third-party service providers to our business to determine if additional services are needed, if the provider is meeting its contractual obligations, or if remedial action is necessary. We may request information from third-party service providers in relation to ML / TF compliance and risk management as part of our internal vendor review process.
- (k) **Compliance Innovation:** We are continuously evaluating non-documentary compliance mechanisms for viability on the Site. This may involve testing compliance tools designed for blockchain platforms, including fraud prevention services and on-chain KYC providers.

- 5.6.2 Users can and are encouraged to provide additional information to rebut any suspensions or blocks arising as part of our ongoing transaction monitoring and customer due diligence processes.

5.7 Reliance on Third Parties to Perform Customer Due Diligence

- 5.7.1 SBX does rely on third parties for elements of compliance with its AML Program, including:

- (a) ID verification (Customer Due Diligence) services;
- (b) transaction monitoring and Enhanced Due Diligence,

but understands that SBX remains responsible for the overall customer due diligence process and any decisions made in relation to a customer.

- 5.7.2 Before appointing any third party to perform a function required for compliance with the AML Program or SBX's ML/TF procedures, the relevant SBX stakeholders will:

- (a) require the third party to complete a supplier due diligence questionnaire, or otherwise provide information relevant to SBX assessing any ML/TF risk it faces with that supplier;
- (b) ascertain the ML/TF obligations and regulation that apply to, the relevant controls that the supplier has in place and how SBX can have visibility of the services to be provided and effectiveness of controls, also ensuring this is captured in the agreement;
- (c) ensure that any record or documentation prepared by the third party in the course of providing ML/TF services that SBX requires for record keeping purposes is owned by, and/or immediately available to SBX (which is also a contractual obligation).

- 5.7.3 In relation to third parties performing CDD services on our behalf, we will ensure that they are able to immediately provide the CDD information we are relying on, and comply with the requirements in 5.7.2 above:

5.8 Reporting of unusual transactions

- 5.8.1 We maintain an unusual activity report and suspicious matter reports (UAR and SMR) process which explains how unusual activity is to be identified, documented

and escalated for review, so that an appropriate senior manager can determine whether a matter needs to be reported, and if so, undertake that reporting.

5.8.2 We will lodge unusual matter report as required by applicable law including where:

- (a) relevant transactions of XCG5,000 or equivalent, where there is cause to presume that transactions are related to money laundering or terrorist financing, transactions made by or on behalf of a person who is named on a sanctions list, or such other matter under law or regulation ;
- (b) we suspect on reasonable grounds that a customer is not the person they claim to be (noting that reluctance to provide CDD is not on its own a suspicion, but failure to verify ID may be);
- (c) we suspect on reasonable grounds that the provision, or prospective provision, of our Services are related to a TF, ML or FP offence, or other criminal offence; and/or,
- (d) a transaction or set of transactions does not appear to have a lawful economic purpose.

5.8.3 Where staff detect unusual activity in relation to a customer, they will prepare an unusual activity report for the Compliance Officer (or delegate) to consider for the purposes of determining whether external reporting is required.

5.8.4 In addition, if a customer is identified as being on a sanctions list or linked to ML, TF, or other criminal activities, we will file an appropriate report with the relevant FIU.

5.9 Anti-Money Laundering Compliance Program

5.9.1 The AML Program has been:

- (a) prepared having regard to the risks identified in SBX's ML/TF risk Assessment;
- (b) factoring in the Regulations and other legislation, adapted to SBX's business and adopting a risk based approach.

5.9.2 The Program outlines the policies, procedures and controls SBX has adopted to mitigate and effectively manage the ML, TF and FP risk identified in its risk assessment, proportionate to SBX's size and nature of business. This includes risk

management practices, internal controls, customer due diligence measures, recording keeping, employee due diligence, employee training program, and how SBX will monitor and manage compliance with its AML Program.

5.9.3 The Program will be reviewed and amended as appropriate on the following events:

- (a) after a risk assessment review (having regard to the changes made in the risk assessment, including new products, jurisdictions or payment methods);
- (b) material change to nature, size and complexity of the SBX business, including customer base;
- (c) to comply with any change in AML/CTF regulation, including any direction of CGA or any other relevant regulatory authority;
- (d) at least annually, regardless of whether any changes are made to the risk assessment.

5.9.4 The AML Program will also be reviewed by an independent person, appropriately qualified and experienced in AML/CTF compliance ideally in the global online casino industry, on a regular basis.

5.9.5 We will maintain records relevant to our ML and TF obligations and compliance with our AML Program, as required by law (for a minimum of five years and for customer records five years after the customer relationship ends).

6. Compliance and Consequences of Non-Compliance

6.1 Staff and any other person to whom this Policy applies should escalate any questions, issues, difficulties or non-compliance with the Policy process as soon as possible to their direct manager or the Compliance Officer.

6.2 Where possible, any minor, accidental or inadvertent failure to comply with this Policy will be addressed by further training and communication to ensure relevant staff are familiar with and understand the correct process so that the non-compliance is not repeated.

- 6.3 Deliberate, negligent or repeated failure to comply with this Policy, or a material non-compliance with this Policy even if unintentional, could cause us to be in breach of our license and be exposed to administrative or criminal proceedings, and may result in disciplinary action up to and including dismissal of employees/contractors, or termination of service providers.

7. Related Information

7.1 External documents

- FATF recommendations
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92)
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)
- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)

7.2 Internal documents

This Policy has been prepared and will be reviewed and updated having regard to our AML Program, our ML/TF Risk Assessment, Risk Assessment Methodology, and various ML/TF policies and procedures.

8. Contact Information

For any questions regarding this policy, please contact:

The Compliance Officer, compliance@sbx.com

9. Policy History

Version	Date	Comments	Approver
1.0	25 May 2025	First version of policy	Aftermath BV Board

10. Policy publication

This policy (as updated from time to time) will be published on sbx.com/terms.

Philip M. Humme

Name: Philip M. Humme

Role: Managing Director obo Allyant group B.V.

Date: October 31, 2025