

Anti-Money Laundering & Counter-Terrorist Financing Statement

1. Company Business Model

Seven Days B.V. (“Weeekly” or the “Company”) is a company incorporated under Curaçao law and is in the process of being licensed under a Curaçao eGaming Certificate of Operation. Weeekly operates a crypto-based entertainment platform offering two core product experiences under the domain www.weeekly.com:

- **Weeekly:** A weekly raffle combined with a casino-style gaming environment. Users buy bundles that provide raffle tickets (entries for USDT prize draws) and Weeekly Coins (a virtual currency used to wager on games and earn raffle tickets within the platform).
- **Weeekly Rivals:** A leaderboard competition based entirely on chance outcomes where all participants start with the same fixed amount of virtual currency and compete during a limited timeframe. The user who achieves the highest ending Weeekly Coin balance through gameplay wins the Rivals USDT prize pool.

All games are played using non-withdrawable in-platform currency (“Weeekly Coins”), while all prize pools are settled in USDT. Participation in real-money prize pools that require deposits is only permitted once users have completed the necessary verification procedures.

Weeekly is available to a global user base, excluding individuals in jurisdictions prohibited under Curaçao licensing rules or applicable international sanctions regimes.

The Company complies with relevant Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) obligations regardless of licensing status.

2. Company Policy Statement

Weeekly (operated by Seven Days B.V.) is not classified as a financial institution under the laws of Curaçao and is therefore not subject to regulatory frameworks that apply to banks, traditional money transmitters, or virtual asset service providers (VASPs) operating in financial sectors.

However, as a licensed gaming operator under the Curaçao eGaming regime, and in accordance with the 2016 National Ordinance and Regulations on the Prevention and Combating of Money Laundering and Terrorist Financing (AML/CFT), Weeekly is firmly committed to preventing the use of its platform for any form of illicit activity, including but not limited to:

- Money laundering,
- Terrorist financing,

- Trade sanctions evasion,
- Criminal concealment or proceeds of crime.

Weeekly applies a compliance-driven framework in line with the standards promoted by the Curaçao Gaming Control Board, the Financial Action Task Force (FATF), and international gaming sector guidelines. These standards are adopted to ensure that the platform operates with integrity and does not serve as a conduit for financial abuse.

To that end, Weeekly's Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) program includes, but is not limited to, the following safeguards:

- Implementation of a formal AML/CTF policy and internal procedures designed to identify, deter, and report suspicious activities;
- Designation of a compliance officer to oversee the effectiveness and enforcement of AML/CTF processes;
- Training and awareness for staff, contractors, and third-party partners involved in onboarding, payments, or monitoring with periodic refreshers to align with emerging risks;
- Internal reviews and, where applicable, third-party audits to ensure the ongoing quality of AML/CTF controls;
- Active monitoring of regulatory and sanction frameworks, including periodic updates based on guidance from the Curaçao Gaming Control Board, FATF recommendations, and global AML developments.

Weeekly recognises its role in protecting the gaming and cryptocurrency sectors from abuse and is committed to maintaining full transparency and compliance with all applicable AML/CTF obligations.

3. What Is Money Laundering and Terrorism Financing?

Money laundering is the process by which individuals or entities attempt to conceal or disguise the origin, ownership, or destination of funds obtained through illegal means. The aim is to make illicit proceeds appear legitimate by passing them through a series of complex transactions or financial layers. This process typically occurs in three stages:

- Placement: Introducing illegally acquired funds into the financial or digital ecosystem (e.g., purchasing cryptocurrency or credits with cash)

- Layering: Conducting a series of transactions to obscure the trail (e.g., transferring between wallets, using anonymizing services).
- Integration: Reintroducing the laundered funds into the economy as seemingly lawful assets (e.g., claiming prize winnings or refunds).

Terrorist financing, while often involving smaller sums, refers to the collection, movement, or provision of funds intended to support terrorist acts or organizations, regardless of whether the source of the funds is legal or illegal.

Weeekly recognises that platforms offering digital currency, remote access, and pseudonymous features may be vulnerable to such misuse. As part of our AML/CTF program, we have implemented:

- Automated transaction monitoring
- Blockchain tracing tools
- Mandatory identity verification (KYC)
- Escalation protocols for suspicious behaviour

These measures are designed to detect, disrupt, and report any activity suspected of facilitating money laundering or terrorist financing.

4. Transaction Monitoring & Risk-Based Controls

Weeekly operates under a comprehensive transaction monitoring and risk-based control framework to detect and prevent money laundering, terrorist financing, sanctions violations, and other forms of suspicious activity. This framework adheres to Curaçao's AML/CFT regulatory standards and international best practices for crypto-based entertainment platforms.

4.1 Real-Time and Periodic Monitoring

Weeekly conducts ongoing monitoring of all user activity, using a combination of automated tools and manual review:

- In-house rule-based systems analyze deposit behavior, wagering anomalies, and game interactions for red flags.
- Third-party blockchain forensic providers (e.g., Chainalysis, TRM Labs) monitor wallet addresses and transactions.

- Manual investigations are launched upon detection of high-risk behavior, system alerts, or external referrals.

Each crypto transaction (deposit/withdrawal) undergoes automatic Chainalysis scanning to detect ties to illicit sources, sanctioned entities, or darknet marketplaces.

4.2 Sanctions Screening and Jurisdictional Controls

Weeekly complies with global sanctions regimes, including those issued by OFAC, the EU, the UK, and the United Nations. We employ:

- Geo-IP tracking and time zone cross-referencing to identify spoofing or use of VPNs;
- Sanctions list screening of wallet addresses and KYC data prior to issuing any deposit address;
- Re-screening of user data throughout the customer lifecycle;
- Flagging or rejecting transactions from U.S.-based exchanges, privacy coins, or mixing services.

Users attempting to interact from prohibited jurisdictions or sanctioned regions may have their funds frozen, account suspended, or be asked to provide supplementary proof of eligibility.

4.3 Detection and Review of Suspicious Activity

Weeekly monitors accounts for red flags, including:

- Unusual deposit and withdrawal request frequency, volume, or routing;
- Gaming activity inconsistent with platform norms (e.g., max bet spam or mirroring behavior);
- Wallets linked to mixing services or obfuscation tools;
- Structuring behavior (e.g., deliberate breaking up of large transactions);
- Links to addresses known for fraud, scams, or high-risk markets.

Such events trigger internal investigation, suspension, and where applicable, the filing of Suspicious Transaction Reports (STRs) with the Curaçao Gaming Control Board or other competent authority.

4.4 Withdrawal Threshold-Based KYC Triggers

Weeekly uses dynamic thresholds to trigger KYC and Enhanced Due Diligence (EDD) before allowing large or repeated withdrawals:

- High-risk users may be asked to provide source-of-wealth and source-of-funds documentation;
- Accounts that exhibit unusually large deposits with limited platform usage may be flagged for further review and required to provide additional information under Enhanced Due Diligence (EDD) protocols before withdrawals are permitted.
- Accounts that submit repeated withdrawal requests within a short time frame may be flagged for further review and, if necessary, temporarily suspended pending investigation.

Thresholds are risk-adjusted based on the user's behavior, jurisdiction, and total platform exposure.

4.5 Anti-Mixing Measures and Wallet Profiling

Weeekly prohibits the use of mixers, tumblers, or other privacy-enhancing tools. In addition:

- Wallets from known decentralized exchange aggregators or peer-to-peer bridges are screened for obfuscation;
- Suspicious transactions are subject to address clustering analysis and blockchain risk scoring;
- Deposits from high-risk wallet types may trigger enhanced review, suspension, or outright rejection.

Weeekly will not onboard funds that have passed through blacklisted services or assets originating from high-risk jurisdictions.

4.6 Advanced Controls: Ban Evasion, Device Matching, and Time Zone Analysis

To detect identity abuse or ban evasion, Weeekly utilizes:

- Device fingerprinting and behavioral analytics to detect linked accounts across the platform;
- Time zone inconsistency checks to identify users attempting to spoof location via VPNs;
- Session-based triggers tied to jurisdiction manipulation attempts or scripting behavior.

Accounts flagged for manipulation are locked pending investigation. Repeat offenders are blacklisted.

4.7 Vendor Oversight and Compliance Innovation

Weeekly performs regular due diligence and performance audits on all third-party compliance vendors and tools. We maintain strict service-level expectations and may:

- Terminate vendor relationships that no longer meet compliance requirements;
- Adjust tools or processes based on regulatory updates, risk shifts, or operational needs;
- Employ emerging technologies to improve anomaly detection and compliance scalability.

4.8 User Obligations

Users agree to:

- Refrain from using mixing services, privacy-enhancing wallets designed to obscure the source of funds, or falsifying identity or location data;
- Cooperate fully with KYC/EDD requests, including providing documentation upon request;
- Use only wallets that they control directly and avoid using shared, pooled, or exchange hot wallets for withdrawals;
- Promptly respond to any compliance inquiries or investigations initiated by Weeekly.

Non-compliance with these obligations may lead to forfeiture of funds, permanent account suspension, and mandatory reporting to relevant authorities, in accordance with our Terms and Conditions

5. User Obligations Under AML & Compliance Rules

To ensure full compliance with applicable Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and sanctions laws, all Weeekly users are required to:

5.1 Provide Accurate Information

- Submit accurate and complete personal information during registration, including name, date of birth, and address;
- Promptly update account information if changes occur (e.g., residency, wallet ownership);
- Use only wallet addresses for deposits and withdrawals that are solely owned and controlled by the account holder, and not shared, pooled, or custodial wallets (e.g., exchange hot wallets)

5.2 Cooperate with Verification Requests

- Comply promptly with all Know Your Customer (KYC) procedures and, if applicable, source-of-funds verification requirements;
- Provide valid, government-issued identification and supporting documents when requested;
- Respond truthfully and in a timely manner to compliance inquiries related to suspicious activity.

5.3 Avoid Prohibited Behavior

Users must not:

- Use Weeekly to conceal or disguise the origin of funds;
- Deposit from or withdraw to wallets associated with sanctioned entities, privacy-enhancing tools intended to obscure source of funds, or third parties;
- Engage in coordinated activity to exploit bonuses, leaderboard outcomes, or referral systems.

5.4 Report Suspicious Activity

- Users are encouraged to report any suspicious or unauthorized activity on their account to support@weeekly.com immediately;
- If you suspect another player is engaging in fraud, collusion, or AML violations, you may report this confidentially to our Compliance Team.

Failure to comply with these obligations may result in account suspension, forfeiture of funds, and mandatory reporting to regulatory authorities

6. Know Your Customer (KYC) Verification

Weeekly is committed to upholding the highest standards of regulatory compliance, anti-fraud controls, and responsible gambling practices. As part of our obligations under the Curaçao eGaming license and global Anti-Money Laundering (AML) frameworks, we implement rigorous Know Your Customer (KYC) procedures before permitting any real-money participation, prize withdrawals, or high-risk user activity.

6.1 Risk-Based Customer Due Diligence (CDD)

Weeekly adopts a risk-based approach to Customer Due Diligence, tailored to the nature and purpose of each user's relationship with the platform. This includes:

- Collecting identity data during onboarding (e.g., email, wallet address, country of residence);
- Screening wallet risk profiles and jurisdictional indicators;
- Maintaining internal records tied to identity, activity, and verification logs;
- Checking against global terrorism, sanctions, and AML watchlists.

KYC thresholds may vary depending on the services used, account activity, or regional requirements — such as total USDT volume, wallet type, or flagged jurisdictions

6.2 Identity & Age Verification Requirements

Before granting access to any real-money prizes or high-risk services, users must complete a KYC process, which includes but is not limited to:

- Full legal name;
- Country of residence and citizenship;
- Government-issued ID (e.g., passport, national ID, driver's license);
- Proof of address (e.g., utility bill, bank statement not older than 90 days);
- Live biometric verification or selfie;
- Source of funds or wealth (in higher-risk cases or flagged accounts).

Verification is conducted through our regulated third-party provider (e.g., Veriff) and may involve biometric tools, document scanning, and sanctions list matching.

6.3 Geo-Blocking and Jurisdictional Screening

Weeekly enforces IP-based geo-blocking and wallet address screening to restrict access from:

- Jurisdictions where online gaming is prohibited;
- Countries subject to international sanctions (e.g., Iran, North Korea, Cuba, Syria, Crimea);
- wallets associated with U.S.-based exchanges or activity indicative of a U.S. person

Users are notified during onboarding that access is prohibited from restricted jurisdictions. Any circumvention (e.g., VPNs, falsified addresses) is a violation of our Terms.

6.4 Ongoing Monitoring & Enhanced Due Diligence (EDD)

All user accounts are continuously monitored using a mix of internal analytics and third-party tools (e.g., Chainalysis) to detect:

- Irregular activity patterns;
- High-risk or flagged wallet sources;
- Rapid turnover of funds inconsistent with typical user behavior.

When red flags are triggered, Enhanced Due Diligence (EDD) may be initiated, requiring users to submit:

- Secondary identity documents;
- Full tax ID, passport, or alternative national documentation;
- Detailed source of funds and source of wealth statements.

Accounts under EDD review may be suspended until sufficient verification is completed.

6.5 KYC Refusal or Failure

Weeekly will not accept or will immediately block users who:

- Fail to provide requested KYC information;

- Submit falsified, expired, or unverifiable documents;
- Attempt to mask location through proxy or VPN;
- Appear on global sanctions or terrorist watchlists;
- Originate funds from blacklisted or high-risk exchanges;
- Are suspected of self-exclusion evasion or mental health risk related to gambling.

We reserve the right to permanently disable such accounts and, where applicable, report users to the appropriate regulatory bodies.

6.6 Timing and Review

- Most KYC requests are processed within 24 hours.
- Verification delays may occur due to document discrepancies or high-risk behaviour.
- Users are notified of any additional steps required during the process.

Most KYC requests are processed within 24 hours. Verification delays may occur due to document discrepancies or high-risk behaviour. Users are notified of any additional steps required and may contact support@weeekly.com for assistance

6.7 KYC in Free-Entry Phase

During free-to-play periods, KYC is not required to participate in games or raffles. However:

- No real-money prizes or withdrawals will be processed without identity verification;
- Users must self-certify they are 18+ before accessing any features;
- Weeekly reserves the right to retroactively require KYC in case of suspected abuse.

7. Governance & Compliance Training

7.1 Compliance Oversight

Weeekly appoints a dedicated Compliance Officer responsible for maintaining AML/CFT policies, overseeing risk management procedures, and ensuring adherence to Curaçao

eGaming regulations. The officer reports to senior management and serves as the primary liaison with regulators and relevant authorities.

7.2 Internal Risk & Oversight

A cross-functional Compliance Committee supports the Compliance Officer by regularly reviewing transaction patterns, emerging risks, and platform vulnerabilities. The committee reviews and may recommend updates to compliance policies or controls based on evolving threats, risk exposure, or legal obligations.

7.3 Staff Training

All relevant employees, contractors, and third-party service providers undergo role-based AML/CFT training:

- Delivered during onboarding and refreshed annually
- Covers red flag detection, KYC workflows, sanctions screening, and escalation procedures
- Completion is logged for audit readiness and regulatory reporting

7.4 Policy Audits & Reviews

Weeekly conducts regular internal compliance reviews and may engage external auditors in response to regulatory developments, incident reviews, or material risk events. All AML/CTF policies are reviewed at least annually, and updates are made in line with legal obligations, risk assessments, and operational feedback

8. Reporting & Recordkeeping

8.1 Suspicious Transaction Reporting

As a platform licensed under the Curaçao eGaming regime, Weeekly maintains formal procedures to identify, investigate, and report activity that may indicate money laundering, terrorist financing, sanctions violations, or other criminal behaviour.

Suspicious Transaction Reports (STRs) are prepared and submitted to the Curaçao Financial Intelligence Unit (FIU) per national AML/CFT laws.

Indicators include, but are not limited to, unusual deposit/withdrawal patterns, structuring behaviour, falsified documents, and use of privacy-enhancing tools.

8.2 Regulatory Cooperation

Weeekly is committed to cooperating fully with competent authorities, including regulators, law enforcement agencies, and financial intelligence units. Where legally obligated, Weeekly will disclose requested information and provide necessary assistance in support of criminal or regulatory investigations.

8.3 Recordkeeping Obligations

Weeekly retains all relevant KYC, transaction, communication, and compliance records for a minimum of five (5) years or as otherwise required under Curaçao AML/CFT laws.

This includes, but is not limited to:

- Customer identification and verification data,
- Deposit and withdrawal histories,
- Internal monitoring alerts and investigation logs,
- Suspicious activity reports and follow-up actions.

All records are timestamped, securely encrypted, and stored in a manner consistent with data protection regulations. Information is made available to regulators or authorities upon lawful request.

9. Additional AML/KYC Compliance Clauses

9.1 User Cooperation & Acknowledgment

By registering and using Weeekly, You agree to cooperate fully with any compliance-related inquiries or reviews. This includes providing accurate, current documentation for identity verification, source of funds, or account activity when reasonably requested.

Failure to cooperate, refusal to provide requested documentation, or attempts to mislead our compliance team may result in the suspension, withholding, or permanent closure of your account, and any associated funds may be frozen pending further investigation.

9.2 Politically Exposed Persons (PEP) and Public Office Risk

Weeekly reserves the right to perform enhanced due diligence on any user identified as a Politically Exposed Person (PEP), including individuals who hold or have held senior political, judicial, military, or administrative positions, or are closely associated with such persons.

PEPs may be required to disclose additional information regarding their source of funds and undergo more frequent transaction reviews in line with international AML best practices.

9.3 Anonymity and Privacy-Enhancing Tools

Weeekly explicitly prohibits the use of anonymity-enhancing technologies such as mixers, tumblers, privacy-focused cryptocurrencies (e.g., Monero), or any tools or methods designed to obfuscate the origin of crypto transactions.

Accounts linked to such behaviour may be suspended or terminated, and funds may be withheld pending a full compliance review. These actions may be reported to competent authorities under Curaçao AML/CFT regulations.

9.4 Periodic Policy Review and Improvement

Weeekly's AML/CFT program is subject to periodic review to ensure compliance with Curaçao law, evolving regulatory requirements, and industry best practices.

Our policies are updated as needed to address new risks, strengthen detection systems, or enhance procedural fairness in response to regulatory guidance or internal audit outcomes.