

Anti-Money Laundering Policy

OnPoint Administration LLC

OnPoint Administration LLC, a Delaware limited liability company ("**OnPoint**," "**we**," "**us**," or "**our**"), owns and operates OnPointCasino.com (the "**Platform**"). OnPoint is firmly committed to preventing the use of the Platform for money laundering, terrorist financing, fraud, sanctions evasion, or any other financial crime. This Anti-Money Laundering Policy (this "**Policy**") describes the key elements of our risk-based anti-money laundering ("**AML**") and sanctions compliance program and explains what we require of every user.

This Policy forms part of, and should be read together with, our Terms and Conditions (the "**Terms**"), Sweepstakes Rules, Privacy Policy, and Refund Policy. Capitalized terms not defined in this Policy have the meanings given in the Terms.

Zero tolerance: OnPoint does not tolerate money laundering, terrorist financing, or sanctions evasion. Accounts involved in suspected financial crime may be suspended or closed, Virtual Coins and pending redemptions may be forfeited, and activity may be reported to law enforcement and other appropriate authorities.

CONTENTS

- | | |
|--|---|
| 01 Purpose and Scope | 10 Suspicious Activity Reporting |
| 02 Legal and Regulatory Framework | 11 Actions We May Take |
| 03 Program Governance | 12 Record Keeping |
| 04 Risk-Based Approach | 13 Training and Independent Testing |
| 05 Customer Due Diligence | 14 Cooperation with Authorities and Partners |
| 06 Enhanced Due Diligence | 15 Your Responsibilities |
| 07 Sanctions and PEP Screening | 16 Changes to This Policy |
| 08 Payment and Redemption Controls | 17 Contact Us |
| 09 Transaction Monitoring and Red Flags | |

01 PURPOSE AND SCOPE

The purpose of this Policy is to establish the controls we use to detect, deter, and report financial crime on the Platform, and to protect our users, our payment partners, and the integrity of our sweepstakes promotions. This Policy applies to:

- All users and Accounts, including all purchases of Gold Coins and all redemptions of Sweeps Coins for Prizes;
- All members, managers, employees, and contractors of OnPoint; and
- Service providers that perform identity verification, payment processing, or compliance functions on our behalf, to the extent of those functions.

02 LEGAL AND REGULATORY FRAMEWORK

Our AML and sanctions compliance program is designed with reference to applicable U.S. federal and state laws, regulations, and guidance, including:

- The Bank Secrecy Act (31 U.S.C. § 5311 et seq.) and its implementing regulations;
- Title III of the USA PATRIOT Act;
- Regulations administered by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") (31 C.F.R. Chapter V);
- Guidance issued by the Financial Crimes Enforcement Network ("FinCEN"); and
- The compliance requirements of our payment processors, banking partners, and card networks.

We also consider recognized international standards, including the recommendations of the Financial Action Task Force (FATF). Where laws or partner requirements differ, we apply the stricter standard.

03 PROGRAM GOVERNANCE

- **AML Compliance Officer.** OnPoint has designated an AML Compliance Officer who is responsible for the day-to-day oversight of this program, including customer due diligence, transaction monitoring, investigations, reporting, record keeping, and training. The AML Compliance Officer has the authority, independence, and resources needed to carry out these responsibilities and reports directly to OnPoint's members.
- **Senior management oversight.** OnPoint's members approve this Policy and receive regular reports on the program's effectiveness, emerging risks, and any significant compliance matters.
- **Policy review.** This Policy and our underlying risk assessment are reviewed at least annually, and sooner when there are material changes to our products, payment methods, applicable laws, or risk environment.

04 RISK-BASED APPROACH

We apply a risk-based approach, meaning that the level of due diligence and monitoring we apply is proportionate to the risk each Account presents. Our enterprise risk assessment considers customer, geographic, product, payment method, and delivery channel risks. Each Account is assigned a risk rating, which is updated as new information becomes available.

RISK LEVEL	TYPICAL INDICATORS	CONTROLS APPLIED
Standard	Verified identity, consistent profile and activity, low purchase and redemption volumes	Customer due diligence and ongoing automated monitoring
Elevated	Higher volumes, frequent payment method changes, unusual activity patterns, or partial risk indicators	Additional verification, closer monitoring, and manual review of redemptions
High	Politically exposed person status, adverse media, significant unexplained activity, or multiple red flags	Enhanced due diligence, senior compliance approval, and possible limits or closure

05 CUSTOMER DUE DILIGENCE

We verify the identity of our users using a tiered approach. We may require any level of verification at any time, and verification must be completed before the activity it applies to is permitted.

STAGE	WHEN IT APPLIES	WHAT WE VERIFY
Registration	When an Account is created	Full name, date of birth, residential address, email address, phone number, age, and location in a permitted jurisdiction
Full Verification (KYC)	Before the first Prize redemption, when risk-based thresholds are reached, or when a risk indicator is detected	Government-issued photo ID, selfie and liveness check, proof of address, and sanctions and PEP screening
Enhanced Due Diligence	High-risk Accounts, significant activity, or unresolved red flags (see Section 6)	Source of funds, source of wealth, and additional documentation, with senior compliance review
Ongoing Due Diligence	Throughout the life of the Account	Continued monitoring, periodic rescreening, and updated documents when information changes or expires

Identity verification is performed with the assistance of a specialized third-party identity verification provider. The name on each Account must match the user's government-issued identification and every payment and redemption method used. Personal information collected for due diligence is handled in accordance with our Privacy Policy.

We will not open or maintain an Account, process a purchase, or pay a Prize where we are unable to complete appropriate due diligence.

06 ENHANCED DUE DILIGENCE

Enhanced due diligence ("EDD") is applied where an Account presents a higher risk of financial crime. EDD may be triggered by, among other things:

- A match or potential match against a politically exposed person (PEP) list, or relevant adverse media;
- Purchase or redemption activity that is significant, or inconsistent with the user's known profile;
- Activity that matches one or more of the red flags described in Section 9; or
- Information from a payment partner, law enforcement, or another reliable source indicating elevated risk.

EDD measures may include obtaining information and documentation about the user's source of funds and source of wealth (such as pay stubs, bank statements, or tax documents), verifying the purpose of the activity, requiring senior compliance approval to maintain the Account, applying purchase or redemption limits, and conducting more frequent monitoring. If a user does not provide requested EDD information within the time we specify, we may suspend purchases, gameplay, and redemptions until it is received.

07 SANCTIONS AND PEP SCREENING

- **Sanctions screening.** Users are screened against OFAC's Specially Designated Nationals and Blocked Persons List and other applicable U.S. government sanctions lists at onboarding and on an ongoing basis as lists are updated.
- **Prohibited persons.** We do not permit any person or entity identified on a sanctions list, owned or controlled by a sanctioned person, or located in or ordinarily resident in a comprehensively sanctioned country or region, to use the Platform.
- **Confirmed matches.** Where a sanctions match is confirmed, we will block or reject the relevant activity and report it to OFAC as required by law.
- **PEP screening.** Users are screened for politically exposed person status and relevant adverse media. A PEP designation does not automatically prevent a user from holding an Account, but it results in enhanced due diligence.
- **Geographic controls.** The Platform is available only to eligible users located in permitted U.S. jurisdictions. We use geolocation technology and prohibit the use of VPNs, proxies, and other location-masking tools.

08 PAYMENT AND REDEMPTION CONTROLS

The structure of the Platform is designed to reduce the risk of misuse. Our payment and redemption controls include:

- **No cash.** We do not accept cash, money orders, or cash equivalents.
- **Own-name payment methods only.** Purchases may only be made with payment methods registered in the Account holder's own name. Third-party, shared, or corporate payment methods are not permitted.

- **Verified redemptions.** Prizes are paid only to a verified redemption method in the Account holder's own name, and only after full identity verification is complete.
- **Play-through requirements.** Sweeps Coins must meet the play-through requirements in the Sweepstakes Rules before they are eligible for redemption, which helps prevent the Platform from being used to move funds without genuine gameplay.
- **No transfers between users.** Virtual Coins cannot be transferred, gifted, sold, or exchanged between Accounts or with third parties.
- **Limits.** We may apply purchase, redemption, and velocity limits based on an Account's risk rating and activity.
- **Digital currency.** Where digital currency payments are offered, we or our payment partners screen wallet addresses and transactions using blockchain analytics tools, and we may refuse transactions linked to sanctioned, illicit, or high-risk sources.

09 TRANSACTION MONITORING AND RED FLAGS

We monitor Account activity on an ongoing basis using automated tools and manual review. Alerts are investigated by our compliance team, and the outcome of each investigation is documented. Activities that may indicate money laundering or other financial crime include:

CATEGORY	EXAMPLES OF RED FLAGS
Purchase and redemption patterns	Purchasing Gold Coins and redeeming Sweeps Coins with minimal gameplay; rapid purchase-and-redeem cycles; activity inconsistent with the user's profile
Structuring	Splitting purchases or redemptions into smaller amounts to avoid limits, reviews, or verification thresholds
Payment methods	Multiple or frequently changing payment methods; payment methods in another person's name; high rates of declined transactions or chargebacks
Multiple Accounts	Accounts linked by device, IP address, payment method, or personal details; coordinated activity across Accounts
Collusion	Users acting together to manipulate gameplay or move value between Accounts
Identity and location	False, altered, or inconsistent documents; reluctance to complete verification; use of VPNs or proxies; locations inconsistent with the user's profile
External information	Negative news, law enforcement inquiries, or alerts from payment partners

10 SUSPICIOUS ACTIVITY REPORTING

Where we know, suspect, or have reason to suspect that activity on the Platform involves funds derived from illegal activity, is intended to evade legal requirements, or has no apparent lawful purpose, we will investigate and, as required or permitted by law, report the activity to FinCEN, law enforcement, or other appropriate authorities.

Confidentiality of reports: Federal law generally prohibits disclosing whether a suspicious activity report has been filed. For that reason, we will not confirm or deny to any user whether a report has been made, and we may be unable to explain the specific reasons for certain Account actions.

OnPoint staff are required to escalate any suspicious activity to the AML Compliance Officer promptly and are prohibited from alerting the user concerned.

11 ACTIONS WE MAY TAKE

To comply with this Policy and applicable law, we may, at any time and without prior notice:

- Request additional information or documentation, and delay or hold purchases, gameplay, or redemptions until it is received and reviewed;
- Apply limits to an Account, or suspend it pending investigation;
- Decline, reverse, or cancel any purchase or redemption;
- Close an Account and, in accordance with the Terms, void Virtual Coins and cancel pending redemptions;
- Refuse to open new Accounts for any person connected to prohibited activity; and
- Report activity to, and cooperate with, law enforcement, regulators, and our payment partners.

These actions are taken in accordance with our Terms. Complaints about Account actions may be submitted under our Customer Complaint Policy, subject to the confidentiality limitations described in Section 10.

12 RECORD KEEPING

We maintain records of customer identification and verification, due diligence and EDD documentation, transaction and redemption history, monitoring alerts and investigations, sanctions screening results, and any reports filed. These records are retained for a **minimum of five (5) years** after the Account is closed or the relevant transaction is completed, or longer where required by law, and are stored securely with access limited to authorized personnel.

13 TRAINING AND INDEPENDENT TESTING

- **Training.** All relevant staff receive AML and sanctions training when they join and at least annually after that. Training covers applicable legal requirements, this Policy, red flag identification, escalation procedures, and the confidentiality of reports.
- **Independent testing.** The effectiveness of our AML program is tested periodically by a qualified party independent of the program's day-to-day operation. Findings are reported to OnPoint's members and remediated promptly.

14 COOPERATION WITH AUTHORITIES AND PARTNERS

We cooperate fully with law enforcement and regulatory authorities and respond to valid subpoenas, court orders, and other lawful requests for information. We also work closely with our payment processors, banking partners, and identity verification providers, and we may share information with them as necessary to prevent financial crime, in accordance with our Privacy Policy and applicable law.

15 YOUR RESPONSIBILITIES

By using the Platform, you agree to:

- Provide accurate, complete, and current information, and update it promptly when it changes;
- Use only funds that belong to you and are derived from lawful sources;
- Use only payment and redemption methods registered in your own name;
- Complete identity verification and provide any EDD information we request in a timely manner;
- Maintain only one Account and never allow anyone else to use it; and
- Not use, or attempt to use, the Platform for money laundering, terrorist financing, sanctions evasion, fraud, or any other unlawful purpose.

Providing false information or attempting to circumvent our controls is a violation of our Terms and may be reported to the appropriate authorities.

16 CHANGES TO THIS POLICY

We may update this Policy from time to time to reflect changes in law, regulatory guidance, partner requirements, or our risk assessment. The "Last Updated" date at the top of this Policy reflects the most recent revision, and the current version posted on the Platform applies.

17 CONTACT US

For questions about this Policy or our compliance program, please contact us using the subject lines below.

REQUEST TYPE	SUBJECT LINE
Questions about this Policy or verification requirements	AML Compliance Inquiry
Submitting requested EDD or source-of-funds documents	EDD Documents
Payment partner or law enforcement inquiries	Compliance Request

ONPOINT ADMINISTRATION LLC — COMPLIANCE

Email: support@onpointcasino.com

Website: OnPointCasino.com