TENNESSEE SPORTS GAMING

VENDOR

PAYMENT PROCESSOR PROCESS

Revised January 8, 2026

Name of Vendor:_____

I. IDENTITY VERIFICATION AND KYC:

1. Describe the Vendor's comprehensive KYC procedures, including the workflow for Player registration, and the process used to match the Player's name to the payment method used.
2. Does the Vendor have the technical ability to block transactions by minors or self-excluded Players? Describe the methodology to identify and prevent access by these individuals.
3. How would the Vendor's system determine that a payment method is linked to an account held by a minor or Prohibited Participant? How would the Vendor alert the Operator to this information?
4. What are the Vendor's controls for geolocation, and how do they integrate with identity verification?
5. Describe the Vendor's process for ensuring that the sportsbooks it works with are licensed in the jurisdictions in which it provides services, and the controls used to prevent the Vendor's services from being used by unlicensed sportsbooks.
6. What information does the Vendor currently receive about Players in Tennessee, and how is that used to verify that the payment details match the Operator's account holder?

II. TECHNICAL INTEGRATION AND CORE SECURITY:

7. Are the Vendor's payment processing services integrated directly into the app (i.e., allowing users to pay without leaving the app), or is the player transferred or redirected to the payment processor's app or web browser to complete the transaction?
    a) If in-app payment processing, apart from federal and state law and regulations, are there any platform payment processing rules or standards that the Vendor must comply with, such as Apple or Google app store requirements?

    b) If transferred out to the payment processing service, does the payment processing service have account security measures in place? For example, account and password sign-in, KYC verification during payment account creation, and MFA when accessing the payment account, etc.?

8. Does the Vendor maintain a formal information security policy, and how often does the Vendor test networks to ensure proper security measures are in place?

III. TRANSACTION MANAGEMENT:

9. Describe the Vendor's methodology to prevent the usage of payment methods prohibited by the state of Tennessee, such as credit cards.
10. Which payment methods (e.g., ACH, debit card, e-wallets) does the Vendor accept for deposits and withdrawals, and what are the usual approval rates seen for each type? Does the Vendor use BIN or IIN filtering to exclude certain types of payments?
11. Describe the Vendor's specific procedures for payment processing services involving cash at retail and assuring the Player is depositing only approved payment methods in Tennessee.
12. What is a typical transaction processing time for deposits and withdrawals? Does the Vendor impose any limits on transaction size or frequency?
13. Does the Vendor delay or enhance deposit processing based on the time of deposit (e.g., right before or during a big game)?

IV. FRAUD PREVENTION AND AML:

14. What are the latest trends the Vendor encounters regarding payment fraud, and what steps are taken to ensure these tactics are detected by the Vendor's system?
15. What are the Vendor's controls for detecting fraud in real time? Does the Vendor's system flag potentially fraudulent transactions and report them to the Operators? How long is the period between identification and reporting of potential fraud?
16. What specific transactional behaviors (e.g., rapid deposit/betting, use of multiple payment types, large deposits) does the Vendor identify as indicative of money laundering or fraud?
17. Does the Vendor utilize any methods to identify problem gambling on behalf of Operators?
18. Describe the Vendor's comprehensive AML policies. Are the AML tools built-in (proprietary) or third-party add-ons?

19. What thresholds or alerts does the Vendor provide to Operators for unusual activity, and at what specific monetary amounts does the Vendor typically flag potential suspicious transactions? Who is notified when this activity is detected, and what is the Vendor's process for reporting unlawful transactions and BSA findings (e.g., SARs, OFAC) internally and externally?

V. REPORTING:

20. Does the Vendor receive a notification when an Operator suspends an account, and how does the Vendor act on that alert to prevent future deposits or withdrawals?
21. How often does the Vendor conduct internal audits of financial controls and KYC controls, and are the results shared with the Operator?
22. Describe the Vendor's protocol for reviewing issues identified by one Operator that may impact others, and the subsequent notification process to alert the other Operators, if any.