



Bet Slip

1 Bet Slip

+ Add more ⚙️

✕ **DEN Broncos**
Moneyline
Broncos @ Colts

+12

\$10.00

Payout: \$12.70

Place Bet \$5.00

Play to Win

The gaming operator's guide
to building safe, profitable
player experiences

OPENING DRIVE

Boost Revenue Without Fumbling on Security

Every moment in the player journey is a revenue opportunity — or a vulnerability. In a highly regulated and competitive industry, gaming operators can't afford to lose good players to friction or let bad actors slip through undetected. At the same time, operators must balance growth with player protection. Supporting responsible gaming means keeping underage or self-excluded individuals off the platform and ensuring high-risk behaviors are detected early.

The key to scaling safely lies in knowing exactly when and how to apply smart, seamless risk controls without getting in the way of a great user experience.

This guide walks through the most critical stages of the player journey, from sign-up to cash-out, highlighting how leading operators are optimizing each interaction to convert more good players, prevent fraud, and maximize lifetime value across their player base.

The Socure Identity Advantage: Seeing the Full Field

The most successful operators think like quarterbacks: they don't just react to where the risk is, they anticipate where it's going. That requires a comprehensive view of identity.

“We are constantly ensuring that we’re leveraging the latest technology, risk models and recommendations from Socure.”

Karl Gambin, VP of Fraud and Payments, Underdog Fantasy

Socure gives operators a unique, 360-degree view of identity through its powerful persistent identifier, SocureID, which connects every signal from phone and device data, to behavioral anomalies, and PII changes into a single dynamic profile. It's how operators shift from reactive to proactive, detecting high-risk behavior patterns long before they result in fraud or regulatory issues.

FIRST DOWN

Maximize Conversions at Sign-Up

First impressions matter. A clunky or slow sign-up experience is all it takes for a player to bounce to your competitor. But gaming operators face a balancing act: uphold responsible gaming practices by verifying age and identity accurately, and still offer a fast, frictionless path to play.

Promotions, like welcome bonuses, can be powerful acquisition tools for fast growth, but they can also be magnets for abuse. Operators need smart defensive strategies to protect against abuse while keeping friction low for legitimate new players.

Smarter sign-ups isn't just about approving everyone. It's about approving more of the right players, including the population of hard to verify next-gen players who drive acquisition volume but are often lost to friction.

What winning looks like

PrizePicks onboarded 1 million players in 10 months and eliminated a 15-person manual review team all while increasing conversions by 10% by automating their verification process with Socure's KYC, Fraud, & Document Verification solution.



What's getting in the way?

Players dropping off during slow or high-friction identity and age verification

Heavy reliance on manual reviews, slowing down onboarding and increasing operational costs

Difficulty verifying 18–25 year olds or thin-file players, leading to lower conversion rates

Inconsistent compliance with KYC, AML, and state-specific rules—putting licenses at risk

How winning operators solve it:

- 01 Simplify the sign up flow with progressive steps and offer a pre-fill sign up experience with minimal inputs like phone or email auto-filling the player's identity information
- 02 Customize onboarding flows by jurisdiction, risk profile, or promo eligibility to reduce unnecessary friction for trusted users
- 03 Leverage AI-driven identity verification that supports broader player auto-approvals and is effective for both mainstream and thin-file populations, including Gen Z (18–24 year olds)
- 04 Implement an intuitive document and selfie capture flow to streamline age verification and comply with KYC requirements

MOVING THE CHAINS

Keep the Drive Alive with Fast, Safe Deposits

The faster the deposit goes through, the sooner they can place bets, play, and generate revenue for your platform. But this step also comes with risk; fraudsters may use stolen bank account details, exploit deposit-based promotions, or attempt to launder money through minimal play and quick withdrawals. Operators need to move fast without opening the door to high-risk funding behavior.

What's getting in the way?

Drop-off caused by slow, redirected, or overly complex funding flows

Fraudsters using stolen, fake, or mismatched account details to deposit funds

Abuse of deposit-based promotions through duplicate or fake accounts

Difficulty verifying accounts tied to neobanks, fintechs, or alternative payment methods

How winning operators solve it:

- 01 Instantly verify bank account status using secure, low-friction methods that don't require logins, redirects, or manual micro-deposits
- 02 Confirm the link between the funding account and the player's identity while also looking for consistency and any signs of previous promo abuse or suspicious activity across other platforms
- 03 Tie funding behavior to the verified identity using device, phone, and email signals, so you can flag anomalies or evolving risk patterns over time
- 04 Ensure your funding workflows can support a wide range of financial institutions, including neobanks and fintechs to minimize drop-off and lost revenue opportunities

LINE OF SCRIMAGE

Make the Right Call for Every Login

Returning players should glide through the login process, especially during high-demand moments like game day or a big tournament. But this critical touchpoint is a notorious hotbed for account takeover (ATO) attempts. Once a bad actor is inside the account, they often make key profile changes — like updating the email, phone number, or password — to lock in control and shut out the rightful owner. Operators need to spot and stop these takeovers without adding unnecessary friction for trusted players.

What's getting in the way?

Stolen credentials used to gain unauthorized access to player accounts

Fraudsters making profile changes (e.g., email, phone) to lock out the legitimate user

Over-reliance on outdated authentication methods (like static 2FA) that frustrate good users

Limited visibility into whether login behavior matches the verified identity

How winning operators solve it:

- 01 Monitor for unusual device, IP, or behavioral signals at login to detect ATO attempts early
- 02 Flag risky profile updates, such as a new email or phone number, by assessing the trustworthiness of the new information in real time
- 03 Trigger re-authentication (e.g., selfie match or one-time passcode) only when risk signals are present, preserving a smooth experience for trusted users
- 04 Continuously evaluate logins and account changes using identity context and behavioral signals

RED ZONE DEFENSE

Secure the Payout

Operators need to ensure that cash-outs are being initiated by the true account holder and directed to a legitimate, verified destination. It's the last mile of trust, and any misstep can result in fraud losses or reputational damage that's hard to recover from.

What's getting in the way?

Bad actors using fake or stolen identities to withdraw funds they were never entitled to

Fraud rings executing low-bet, high-volume strategies to launder funds

Uncertainty about whether a withdrawal request is tied to the same verified player who originally signed up

Operational bottlenecks and payout delays caused by manual review queues

How winning operators solve it:

- 01 Require step-up authentication (e.g., selfie re-verification or trusted device check) before withdrawal if the account shows signs of elevated risk
- 02 Evaluate withdrawal behavior in context, looking at changes in device, behavioral patterns, or new accounts added since initial deposits were made
- 03 Passively screen recipients against sanctions lists or watchlists to prevent unauthorized disbursements
- 04 Monitor withdrawal patterns and velocity to detect signs of mule activity or coordinated laundering schemes

HALF-TIME ADJUSTMENTS

Stay Ahead of Evolving Risk

A player who clears onboarding might later appear on a sanctions list, watchlist, or self-exclusion registry. But many operators struggle to detect these changes quickly enough to respond. When systems are siloed or alerts are delayed, teams lose precious time — and bad actors take advantage. Staying ahead means continuously monitoring risk signals and reacting in real time, before small issues become big losses.

What's getting in the way?

Lack of continuous monitoring for high-risk behavior or status changes

Lack of visibility into real-time shifts in a player's associated PII, risk status, or reputation

Delays between risk events and action due to fragmented systems or manual processes

Siloed systems that miss high-risk patterns across the player lifecycle

How winning operators solve it:

- 01 Leverage a dynamic, persistent identifier for a 360-degree view of identity and an up-to-the second view of player risk
- 02 Enable proactive notifications that trigger alerts for instances such as risky profile changes, or a player is added to a sanctions list Monitor for unusual patterns like login frequency, location changes, or device switches that could signal evolving risk
- 03 Centralize risk signals across systems to reduce response delays and empower teams to act immediately when risk shifts
- 04 Set thresholds and triggers that automatically escalate review or restrict activity when risk signals exceed a defined limit

POST-GAME RECAP

Socure is the MVP that Helps Operators Win

Socure partners with leading gaming operators to help them convert more good players, stop fraud at every stage, and build seamless, trusted experiences that scale.



Here's what success with Socure looks like

Underdog

300% manual review reduction

↓ reduced friction during peak traffic

97% auto-decisioning on ID verification

Prizepicks

10% lift in conversions

↓ eliminated a 15-person manual review team

1M new players onboarded in under 10 months

Top Sportsbook & DFS Operator

59% lift in auto-approvals

40% drop in manual reviews

\$18M+ in incremental LTV by onboarding faster with fewer fraud losses

POST-GAME RECAP

Socure is the MVP that Helps Operators Win

From sign up through cash-out, Socure helps you:

- ✓ Spot and stop fraud before damage occurs.
- ✓ Convert more good players with less friction.
- ✓ Build seamless, compliant, delightful customer experiences across jurisdictions.

Socure's RiskOS™ platform brings it all together with powerful identity verification, fraud signals, and real-time decisioning to support safe, responsible growth across the entire player journey.

RiskOS value to gaming operators:

- ✓ Centralized no-code, drag-and-drop workflows for onboarding, funding, login authentication, and withdrawal
- ✓ Provides total visibility into how and why decisions are made — with the ability to adjust in real time
- ✓ Empowers complex decision logic effortlessly using an intuitive drag and drop canvas
- ✓ Allows for custom alert queues enabling focused and efficient case management

We know what it takes to win, and we're here to support you every step of the way.

Let's build your playbook for safer, smarter growth today.

[Learn more →](#)

Socure is the leading provider of digital identity verification and fraud prevention solutions, trusted by the largest enterprises and government agencies to build trust, reduce friction, and eliminate fraud across the globe. With coverage across 190 countries and 2,800+ customers—including 18 of the top 20 banks, the largest HR payroll platforms, more than 30 government agencies, and over 500 fintechs—Socure delivers industry-best accuracy, automation, and capture rates.

Following its acquisition of Effectiv, Socure now offers end-to-end identity fraud and payment risk management, with advanced capabilities in transaction monitoring, credit underwriting, and know-your-business (KYB). Leading organizations including Capital One, Citi, Chime, Gusto, Robinhood, DraftKings, and many more trust Socure to power digital trust in onboarding, authentication, payments, account updates, and compliance.

