

# ONLINE GAMBLING

Building a safer gambling platform that consumers trust



The popularity of online gambling is a growing global phenomenon. The amount of money exchanging hands in this sector is not escaping the notice of fraudsters, who are targeting it with increasingly complex attack methods.

As consumers increasingly gamble across devices, operators are faced with the challenge of providing an online platform which not only offers users a differentiated customer experience, but also delivers on safety and compliance. To facilitate meaningful engagement on their platforms, operators must identify and stop all fraudsters before they can pollute the online gambling ecosystem.

## Arkose Labs Solution for Gambling Operators

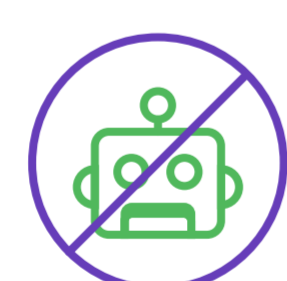
Arkose Labs protects gambling platforms from large-scale fraud attacks and malicious automated traffic. While trusted users can interact with the platform unchallenged, fraudsters are presented with targeted authentication which is tailored to their risk profile.

The Arkose Labs Fraud and Abuse Prevention Platform uses continuous intelligence to assess the risk associated with each user and presents adaptive challenges to risky traffic, stopping fraud. Its unified approach evolves with changing attack patterns and keeps good user experience front and center in order to support customer engagement levels on gambling applications.

The platform is based on two interconnected components — Arkose Detect and Arkose Enforce. Arkose Detect is a dynamic risk engine that analyzes data from live user sessions to feed real-time insights into Arkose Enforce, the challenge-response mechanism. Arkose Detect uses deep device and network forensics, behavioral analytics, continuous intelligence, and historical attack pattern calibration to detect even the most subtle signs of fraud. Traffic is triaged based on its risk profile and Arkose Enforce presents dynamic challenges that increase in complexity with the risk of the user.

Arkose Labs' innovative enforcement challenges negate the risk of defenses being scripted around at scale. While genuine consumers find the challenges fun and simple to complete, fraudsters are forced to spend more time and resources to clear the challenges at scale. This slashes their return on investment, compelling them to abandon attacks.

## Solution Highlights



### Eliminate all automated attacks

*Online gambling companies are targeted with high volumes of basic automated attacks as well as more sophisticated trained bots.* Arkose Labs' unique Acid Test differentiates between all human and automated traffic with tailored challenges that cause automated attacks to spontaneously fail.



### Prevent chip dumping and collusion

*Online gambling platforms are vulnerable to collusion in multi-player games and chip dumping, when criminals use the platforms to move money.* Arkose Labs provides insight into suspicious device identifiers and user behavior combined with friction to deter cybercriminals from targeting the platform.



### Detect new account fraud and bonus abuse

*Many gambling sites offer free bets for new customers, so the onboarding process is a critical touchpoint.* Arkose Labs' platform detects fake new users using stolen or synthesized credentials, providing independent identity insights and fraud data crowdsourced from a global network.



### Protect against account takeover

*Hacking into account enables fraudsters to steal winnings, compromise payment and identity credentials and carry out abuse from trusted accounts.* Arkose Labs adds a powerful layer of security into the account login stage, protecting against credential injections and mass logins from sweatshops.

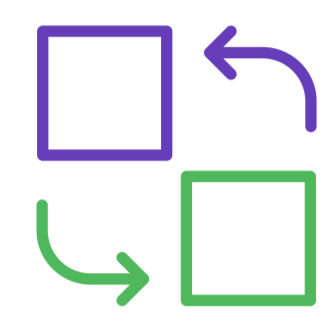
# The Arkose Advantage

The Arkose Labs Fraud and Abuse Prevention Platform enables gambling operators to provide a trustworthy and secure online experience.



## Zero-tolerance to fraud

Stem the rising tide of fraud targeting online gaming platforms by undermining the financial incentive behind large-scale fraud attacks.



## Shift the attack surface

Arkose Labs moves the attack surface away from the online gambling platform to its own network to provide a buffer between businesses and fraudsters.



## Unique visual challenges

Exceptional resilience to large-scale attacks without harming good users' experience.



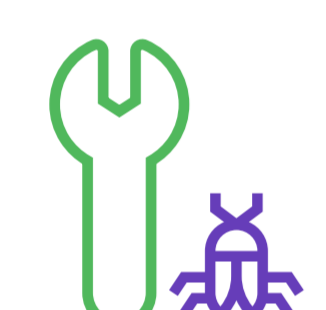
## Self-learning platform

The only platform with a direct feedback loop between risk decisioning and enforcement results, allowing for continuous refinement of risk assessments and the ability to evolve with changing attack patterns.



## Long-term defense

Adaptive defense protocols erode the profitability of attacks which renders fraud economically unsustainable in the long-term.



## 100% attack remediation SLA

Arkose Labs is the only company to offer a guarantee on protection against all automated attacks.

## Promo Abuse in Sports Gambling

Ever since sports gambling was legalized throughout the U.S. in the summer of 2018, gaming operators have flooded the market with digital options. This has led to massive, cutthroat competition among dozens of sports betting firms to win share of the burgeoning U.S. market. One common way these firms attract new customers is to offer promotions: for example, a free matching bet "on the house" for new customers worth whatever amount they initially deposit. Fraudsters have turned this into a goldmine. They will abuse these promotions by depositing money to get the free bet; then cashing out the money immediately. They create new accounts at massive scale using automation to do this many times over, thus stealing large amounts of money from the betting sites and abusing their original intent of new customer acquisition.

## Results

- **Eliminate all automated attacks** on gambling platforms.
- **Increase good customer** throughput by 15-25%.
- **Reduce fraud** by 50-90%.
- **Render fraud attacks** financially non-viable by eroding the return on investment.
- **Protect the brand** of the gambling platform by ensuring a safe user experience.

## Conclusion

Online gambling operators trust Arkose Labs to provide them with a long-term fraud prevention approach which bolsters their defenses and makes them less attractive to fraudsters. To complete Arkose Labs' unique authentication challenges at scale, fraudsters must invest significantly more time and resources as they are unable to script around this defense. As a result, their costs increase while returns keep diminishing, causing fraudsters to abandon the attack and move on. This allows platform operators to offer meaningful engagement to their consumers in a safe gambling environment, helping with long-term commercial success.

demo@arkoselabs.com  
(800) 604-3319  
arkoselabs.com

Schedule  
Demo

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.