How Arkose Email Intelligence Stopped Mass Fake Account Creation in Gaming

A leading global gaming company, renowned for its vast user base and popular titles, faced a critical threat: mass fake account creation undermining game integrity and user experience.

The Challenges

Volumetric Attack Surges: Fraudsters created massive bursts of fake accounts using email variations (e.g., adding "+1", "+2", "+3") from the same IP, overwhelming registration systems and evading traditional detection.

Low-and-Slow Evasion: Fraudsters slowly accumulated fake accounts over time to avoid triggering alarms, allowing undetected abuse for extended periods.

No Email Validation: Lack of email verification allowed fraudulent addresses (from nonsensical handles to completely invalid domains) to slip through unchecked.

Linguistically Ambiguous Addresses: Attackers exploited characters or formats valid in some regions but not others, making invalid registrations difficult to detect.

The Arkose Labs Solution

Integrated Email Intelligence: Deployed Arkose Email Intelligence as an add-on within the broader Arkose Titan platform, enabling unified defense by correlating email data with device and IP signals—addressing a key gap in standalone solutions.

Multi-Vector Risk Analysis: Analyzed 40+ signals across seven vectors in real-time to assess email address risk instantly, catching throwaway, disposable and alias addresses before account creation.

Scalable Detection: Maintained effectiveness even during registration surges of up to 500%, adapting to both volumetric bursts and low-and-slow tactics.

Holistic Platform Defense: Seamlessly integrated email validation with bot management and behavioral intelligence for comprehensive fraud mitigation across the user flow.

Business Results

8M+ Fake Accounts Blocked Annually: Detected and prevented over 8 million fraudulent registration attempts using Arkose Email Intelligence.

24% Lift in Fraud Detection: Achieved 24% additional fake account detection beyond core bot management, flagging 58% of total registration traffic as potentially fraudulent.

Protected Major Email Domains: Stopped high volumes of attacks across Gmail, Outlook and Hotmail, preventing fraudsters from exploiting common providers.

Preserved Account Integrity: Eliminated downstream fraud and platform abuse, protecting both reputation and user trust while maintaining seamless experience for legitimate players.

SCHEDULE CALL WITH AN EXPERT

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.