Fintech Blocks 90% of Fraudulent Accounts and Saves Critical Partner Relationships

A leading fintech platform facing escalating fake account creation that threatened both platform integrity and key business partnerships. Sophisticated attackers were exploiting the registration flow using email-based tactics specifically engineered to evade traditional security controls.

The Challenges

Low-and-Slow Account Creation: Fraudsters created fake accounts gradually over time to stay below volume-based detection thresholds.

Email Enumeration and Tumbling: Attackers generated systematic email address variations and alias techniques to create multiple accounts while appearing legitimate to conventional fraud tools.

Domain Exploitation: Bad actors registered new domains specifically for abuse, using recently created addresses that looked valid but carried high fraud risk – a tactic existing controls weren't built to catch.

The Arkose Titan Solution

Arkose Email Intelligence Added to Existing Stack: Customer gained multi-vector email risk analysis that evaluated formation patterns, gibberish handles, enumeration sequences, domain age and velocity signals in real time.

Domain-Based Risk Controls: Domain intelligence assessed registration dates and ownership signals, flagging the newly registered domains fraudsters relied on as a primary attack vector.

Validated via Fraudulent Session Testing: Before full deployment, the customer tested Email Intelligence against sessions identified as fraudulent and confirmed effectiveness.

Integrated Multi-Layer Defense: Email Intelligence operated in concert with Arkose Titan's bot detection, device identification, behavioral biometrics and IP intelligence for comprehensive coverage across attack vectors.

Business Results

90% of Fraudulent Email Addresses Detected and Blocked: The vast majority of fake accounts were flagged before they could be created, stopping abuse at the source.

70% Caught by Domain Age Controls Alone: The single highest-impact signal was domain intelligence, reflecting how heavily attackers relied on newly registered domains.

Partner Relationships Protected: By shutting down the fraud pipeline overnight, the company preserved trust with key business partners whose relationships were at risk.

No Friction Added for Legitimate Users: The detection layer operated silently for good users, maintaining a seamless registration experience throughout.

> "The multi-layered approach of Arkose Labs gives us visibility we've never had before. Email Intelligence fills a critical gap in our defenses against sophisticated fraud attempts."
>
> — Security Team Lead

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.