Arkose Labs

Online Dating Platform Ghosts Lone Fraudsters Using Arkose Labs Platform

CASE STUDY

Customer: A global dating platform

Business Problem

- Fraudulent new account creation leading to human-driven abuse
- Account takeover and abuse of dormant accounts to escape detection
- Customer dissatisfaction due to disruption in user experience

Solution

Arkose Labs Fraud and Abuse Prevention platform's real-time decisioning could detect bad actors in real-time, while adaptive step-up enforcement challenges sapped their efficiency to protect the dating platform from abuse and preserve the experience of genuine customers.

Results

- 80% reduction in fake account registrations
- Stopped downstream spam and abuse
- Safeguarded interests of genuine customers

Using Arkose Labs data, we can identify and shadow ban malicious users to stop them from abusing our users, which makes the platform safer and increases trust.

- Product Manager

Overview

As online dating becomes the new normal across an increasingly wide demographic range, there are estimates that 32% of all internet users now use dating sites and apps. Users are looking to meet potential matches in a simple and seamless way that fits into their busy lives.

The client is a large online dating platform which makes it quick and easy for users to set up profiles using their photos and a small bio. Prioritizing a smooth on-boarding experience helps ensure they can maintain a wide pool of potential matches for its users which has led to its popularity and rapid global expansion.

The Business Problem

The popularity and simplicity of the client's platform made it a prime target for fraudsters. Specifically, there was a recurring issue where bad actors created fake accounts and proceeded to scam others on the platform. With little information needed to create a profile, fraudsters would create multiple accounts and proceed to send messages to real users on a large scale, inviting them to click malicious links, ask for money or engage in phishing schemes. The company also faced affiliate fraud as well.

The platform wanted to preserve the customer experience and ease of use that it was known for, while at the same time rooting out the creation of these fake accounts. While fraudulent activity could ultimately be identified downstream, they needed an additional line of defense that proactively monitored the account registration stage in order to prevent subsequent abuse. Doing so was critical to retaining user trust and avoiding damage to the brand. This also needed to be achieved with no negative impact on good customer throughput, preserving the quick and easy sign up process.

The Arkose Labs Solution

Targeted, human-driven fraudulent activity is notoriously difficult to detect early. Deploying Arkose Labs at the account registration stage had an immediate positive effect, with the dating company able to identify bad actors early on.

Using advanced behavioral analytics to identify telltales of fraudulent activity enabled the platform to target suspicious traffic with additional friction at the account creation stage. That meant fraudsters were faced with a greater effort to complete each registration. This disincentivized them from creating fake accounts.

Additionally, Arkose Labs passed data signals back to the platform that helped identify returning fraudsters with a high degree of accuracy. The company could also use these insights to ban bad users and identify them if they returned to the platform later, thus reducing future abuse.

This approach successfully thwarted both automated and targeted attacks by fraudsters before they could connect with genuine users to scam them.

Through data sharing with Arkose, we saw double digit improvement week over week in the number of registrations we were able to identify as fraudulent. They have helped us catch 80% of the fraudsters before they can send out messages to genuine users.

The key features of the bespoke solution that Arkose Labs deployed for the company are:

Deep Forensics:

The Arkose Labs solution collects and analyzes digital intelligence, including data from the originating devices, networks, and locations to gain insights into individual user profiles.

Continuous Intelligence:

The solution combines the insights with behavioral analytics to accurately understand the underlying intent and the associated risks of the users to assign risk profiles to every user.

Enforcement Challenges:

The Arkose Labs solution then presents enforcement challenges to activity deemed suspicious, in order to filter out bots and organized sweatshops from genuine users. The insights from Arkose Detect combined with the risk assessment of the user informs Arkose Enforce to present stepped-up challenges for users with higher associated risk. While genuine users—98.6%— can easily clear these challenges, fraudsters must spend more time and resources.

On-brand:

The enforcement challenges are custom-created using the platform's branding in order to blend with the overall user experience and minimize disruption.

The data from user sessions is fed back into Arkose Detect, which provides in-house fraud teams with the required insights to adapt to the evolving attack types and future-proof their fraud prevention approach.

This multi-level, unified approach enables the company to effectively reduce automated as well as targeted attacks and provide a safe online dating environment to users around the globe, without compromising on their online experience.

Long-term Success:

Arkose Labs believes that combating fraud and abuse requires a solution rooted in the prevention of abusive attacks at the point of entry without impacting good customer experience. The adaptive stepped-up enforcement challenges require incremental time and effort from the fraudsters. This continual increase in costs, renders the attacks inefficient and economically non-viable, stopping the cat-and-mouse game that fraudsters play with businesses.

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.

Schedule Demo

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