

# PAYMENTS FIRM FOILS GIFT CARD FRAUD WITH ARKOSE LABS

CASE STUDY



## Major gift and prepaid card provider

### ⚠️ Business Problem

- Large-scale attacks from fraudsters checking card balances and redeeming stolen gift cards
- Persistent attacks from both bots and human fraud rings
- Existing solution (reCAPTCHA) not only failed to stop all attacks but created a bad user experience

### 💡 Solution

- Arkose Labs platform accurately detected good users from bots and human sweatshops (fraud rings)
- Step-up enforcement challenges stopped bots entirely and sapped the efficiency of human sweatshops
- Rich insights enabled the company to share data across teams, creating a more holistic approach to fighting fraud

### ✅ Results

- Vastly improved experience compared to previous solution (reCAPTCHA)
- 98% reduction in bot attacks
- 60% reduction in human-driven fraud

*"The Arkose Labs team is flexible, easy to work with and a true partner in helping us solve fraud issues. They're always available whenever needed and willing to work with us on any use case we have."*

*-VP, Risk Management*

## Overview

The client is one of the premier distributors of prepaid card and gift card programs, with more than 700 partners across its networks in more than 25 countries. The company has grown rapidly and has engaged in partnerships and created innovative solutions to enable gift card use in the digital realm. It is highly trusted and respected by retailers and consumers alike.

## The Business Problem

As one of the largest players in the gift card space, the company found itself the frequent target of fraud attacks. Fraudsters particularly like abusing gift cards and prepaid cards because they are almost like cash and can be extremely hard to trace.

The company had been using reCAPTCHA for authentication, but the legacy solution proved lacking in several areas. Its static, automated images can be easily bypassed by bots using machine vision technology. At the same time, good users faced unnecessary friction. As such fraudsters were able to successfully carry out attacks at scale, from checking the balances of stolen gift cards to redeeming them online.

At the same time, the blackbox nature of reCAPTCHA made it impossible for the company to get any context and insights to assess risk levels across its network and deploy proper resources or scale risk thresholds as needed.

They needed a more robust solution, one that would not only stop even the most cutting-edge bots and persistent humans, but that also provided insight across its entire network of thousands of sites.

# The Arkose Labs Solution

After much due diligence, the company selected Arkose Labs to stop these fraud attacks and saw an immediate reduction in both automated and human-driven fraud with no impact on good customer throughput.

That's because the Arkose Labs platform seamlessly combines best in class intelligence and analytics with adaptive step-up challenges that are designed against the latest in machine vision technology, meaning even the most advanced bots can't solve them. At the same time, human fraud rings that attack sites are identified and fed increasingly complex challenges so that they give up their effort entirely.

Beyond that, Arkose Labs provided the client with actionable insights into fraud patterns, how to stop them, and where best to focus resources in order to be able to change parameters quickly as threats evolved. Arkose Labs was also able to deliver custom metrics as requested and was highly responsive to meet any new requests. The client's internal fraud team was also able to easily share data with its internal risk team, which wasn't possible before using reCAPTCHA. This allowed the company to operate in a much more agile manner to combat fraud attacks. This success led them to further the engagement and deploy Arkose Labs on more than a hundred sites.

## Demonstrated Results

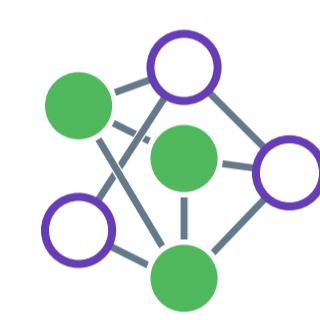
Mere weeks after being deployed, Arkose Labs had already stopped the amount of successful automated attacks getting through by more than 98%. Human-driven fraud was also reduced by more than 60%.

Just as importantly, good users were not faced with an onerous authentication experience that required them to meticulously click on different images. The end result was a safer and more user-friendly experience across the client's ecosystem.

*"We needed a more robust solution; we weren't getting any insights into the data with our old solution. Arkose Labs provided us with custom data and insights that we can share across teams internally."*

”  
-CISO

## Key Advantages



**Powerful Remediation:** Challenges on the Arkose Labs platform can not be solved by automated scripts.



**Managed Services:** Arkose Labs works closely with your business to offer customized, actionable insights.



**Continuously Learning Platform:** The Arkose Labs platform constantly evolves to adapt to emerging threats.



**Seamless Customer Experience:** Good users are never blocked, which eliminates the false positives that hinder customer experience.



**360 Degree Fraud Prevention:** The platform defends your business against spam, fake reviews, denial of inventory, new account origination, account takeover and other complex attacks.

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