

# Fastest Growing Fintech Stops BNPL Fraud with Arkose Labs

CASE STUDY



## Customer:

The fastest growing fintech company in Europe

### Business Problem

- Large-scale automated attacks led to ATOs and fake account creation
- Needed a security solution that could scale fast with company growth

### Impact

- Bot attacks were hurting their brand reputation due to high security expectations of financial services companies
- Attacks led to issues with company's compliance standards and regulations
- Previous solution used a block & accept approach that was not able to keep up with the company's rapid growth

### Results

- Arkose Labs stopped ATO & fake account attacks
- Able to provide attack prevention without hindering customer throughput during high-growth phase of the company

## Overview

The buy now, pay later (BNPL) industry is one of the fastest growing industries today, becoming highly popular in Europe and continuing across the globe. The company offers BNPL services across easy-to-use website and mobile applications where customers only have to pay 25% of what they owe up front, and pay the rest in installments with zero interest.

After accumulating success in Europe, the company has expanded their efforts to other regions, driving growth of millions of customers worldwide in a matter of weeks.

## The Business Problem

The client offers their customers the option of paying in installments using a virtual Mastercard system. However, fraudsters constantly aim to find new vulnerabilities in digital payment systems and have directed their efforts toward the company's customers by launching ATO attacks and creating fake accounts to rip-off merchants.

These large-scale attacks were disrupting the user experience and damaging the company's brand reputation in an industry that expects the utmost security for their customers. These fraudulent transactions continued to happen at scale on the client's platform which threatened the company's ability to remain compliant and operate successfully. The company's previous security solution opted for a binary block & accept technique which hindered the company's ability to scale at the rate that they expected as their business expanded to other regions.

# The Arkose Labs Solution

As the company continues to scale and accept new customers from around the world, Arkose Labs delivers a solution that grows with their increasing rate of transactions. Arkose Labs helped the company from a binary block & accept method of authentication to a dual detection & enforcement challenge system that was able to protect them from large-scale sophisticated bot attacks. Additionally, Arkose Labs provides a managed services platform where the company's transactions are monitored by our 24/7 SOC team for instant alerts and threat metrics.

Arkose Labs was placed on the login and new account sign up flows to protect any ATO attempts or fake account creation. By monitoring hundreds of millions of transactions, Arkose Labs is able to prevent these attacks from sliding by defense initiatives while maintaining the positive, easy-to-use experience the company is known for.

With the BNPL industry still being relatively new to the western world, the Arkose Labs global network of data has provided the visibility BNPL companies need into the wide range of attack telltales and patterns seen across other industries. This network of data has empowered the company to be strides ahead of known and future attack tactics before they happen on their platform.

## Demonstrated Results

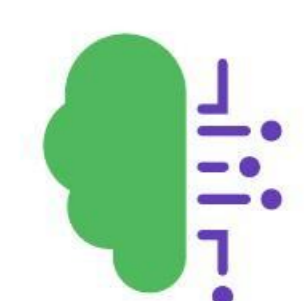
Zilch has been able to successfully prevent these large-scale automated attacks from achieving ATO and fake account creation at scale. Arkose Labs provides assurance for a highly secure financial platform without hindering the good user experience. Arkose Labs has also been highly flexible in maintaining a solid security posture that is adaptable to high growth periods and large quantities of customer transactions.

## The Arkose Labs Advantage



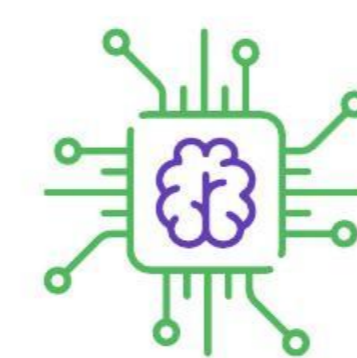
### Adaptive Decisioning:

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



### Continuous Intelligence:

Once combined with behavioral analytics, these insights help determine the underlying intent of the user, and the associated risk level is ascribed.



### Real-Time Challenges:

These are images presented in real-time, designed specifically to foil machine vision technology. The challenges are continually being updated and new ones regularly created.



### Seamless Customer Experience:

Good users are never blocked, which eliminates the false positives that hinder customer experience and drain revenue.

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication", the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput.

Schedule  
Demo

demo@arkoselabs.com  
arkoselabs.com