

Micro-Deposit Fraud: How Arkose Labs Stands Behind Financial Services

The industry of fraud is constantly creating more sophisticated forms of attacks in order to catch businesses off-guard. Micro-deposit fraud is a seasoned attack strategy that has recently resurfaced and is heavily impacting the financial services industry, which calls for an effective solution to help companies improve their fraud deterrence efforts.

Fraudsters have been taking advantage of micro-deposits issued by online banks, fintechs, and payment companies which are used in the process of account verification. Micro-deposit fraud is where attackers create fake accounts to transfer funds, sometimes using stolen credit card information, to make mini deposits under \$1 and as low as \$0.02 to a bank account created separately. They will do this hundreds of times per day over the course of many years, during which the monetary value adds up to a multi-million dollar scheme.

Micro-Deposit Fraud Burdens Financial Institutions

While each transfer only costs a few cents, micro-deposit fraud adds up over time causing a plethora of downstream problems such as added costs and a bad reputation with customers and merchants.



Repayment Costs

Although these deposits are miniscule, the costs add up over time which can lead to a hefty repayment



Increased ACH Fees

Fraudsters making micro-deposits at scale causes added costs in payment processing



Risking Good Standing with Creditors

If the amount of chargebacks exceed the allotted limit set by credit card companies, businesses could lose the right to make online payments altogether



Damaged Customer Relationship

If a customer is a victim of a micro-deposit scam, financial services companies may appear untrustworthy and risk damaging customer relationships



High KYC & CAC Costs

Costing companies hundreds of millions per year, know your customer and customer acquisition costs have become increasingly expensive

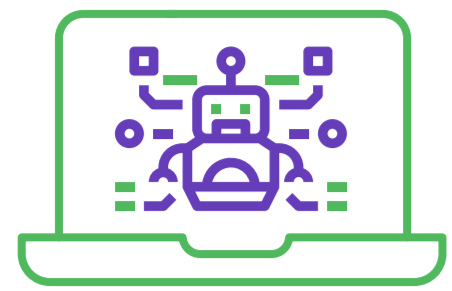
Arkose Labs' Proven Protection Against Micro-Deposit Fraud

Arkose Labs works with global financial services and fintechs to stamp out micro-deposit fraud. The Arkose Labs platform is centered around an AI-driven decision engine that triages suspicious traffic while allowing good users to seamlessly and securely pass through. Arkose Detect determines user intent and risk classification by comparing real-time signals of traffic to our global network of data. Traffic classified as high-risk in our detection platform is administered a curated enforcement challenge. These challenges will cause bot traffic to fail, and incrementally increase the time for human fraudsters to solve, making micro-deposit attacks against our customers unworthwhile. Our flexible solution can plug into critical user touchpoints on websites and mobile apps that are targeted to carry out this form of attack.

1. New Account Registration: Arkose Labs is highly effective at preventing bad actors and bots from setting up fake new accounts at scale, which is the root of micro-deposit fraud

2. Financial Account Management: Arkose Labs provides dynamic protection within websites and apps, through the process of adding and verifying financial account details

Arkose Labs Increases Costs and Sabotages Attacks



Real-Time Decisioning

Arkose Labs distinguishes user traffic by analyzing the behavioral biometrics of a user when interacting with an online platform. Using behavioral biometrics such as keystroke and swipe patterns, our decision engine can decipher between human and bot activity. Suspicious traffic is then filtered out and assigned a curated challenge to prevent attacks. Data is then stored in our global network where future attacks can quickly be diagnosed and no new threats go unnoticed.



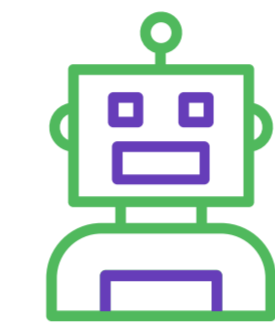
Human-Attack Challenges

Micro-deposit fraud is contributing to the rise in human-driven attacks led by persistent human fraud rings. This calls for specialized challenges to ward off attacks. By making our human fraud challenges time sensitive, fraudsters are unable to successfully solve them and meet the time threshold for their attacks to be financially worthwhile. Human fraudsters abandon attacks on the Arkose Labs platform due to the depletion of their ROI.



Arkose Labs Global Network

Fraud profiles and telltale signs are collected from and shared by other financial services companies in our network which allows for a wider opportunity for fraud deterrence. When other attacks are registered within our network, your company becomes further protected from increasingly sophisticated fraud strategies such as micro-deposit fraud.



Guaranteed Bot Defense

Automated attacks are a continuing problem for businesses due to their ability to attack at scale. Arkose Enforce is capable of completely stomping out bot attacks by administering anti-automation challenges that computer vision technology is incapable of recognizing nor learning how to bypass.

The Arkose Advantage



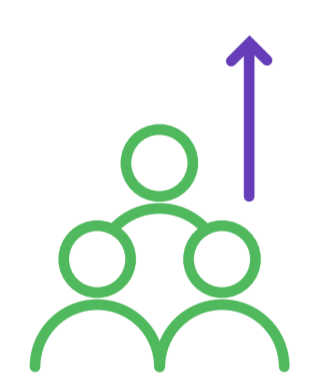
Long Term Deterrence

Arkose Labs increases the cost of fraud making it economically unsustainable to fulfill attacks



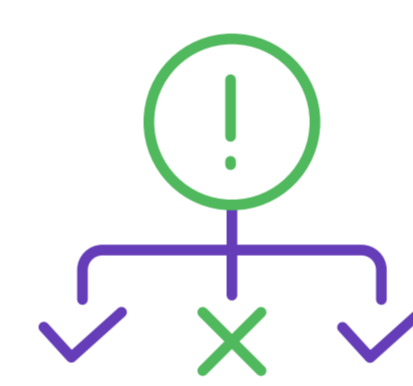
Results Fast

New customers will see results within days, not weeks or months



Guaranteed Efficacy

Powerful protection backed by commercial assurance and industry-first limited warranty



Flexible & Adaptable

One solution that protects against different attack vectors and extensive user touchpoints



Early Detection

Eliminate losses, reduce costs, and streamline efforts by preventing attacks before they advance in your ecosystem



Solving False Positive Conundrum

Legitimate consumers are never blocked and rarely experience user interdiction

Conclusion

The goal of fraud is to spend as little time and money as possible for the highest potential monetary gain. In order to combat this, Arkose Labs removes the financial incentive behind attacks by making it extremely time consuming and expensive to the point where fraud on our platform becomes worthless to cybercriminals. In a frequently targeted industry such as financial services, Arkose Labs strengthens companies by removing the obstacle of current and future forms of fraud like micro-deposits, helping our customers achieve greater success.

demo@arkoselabs.com
(arkoselabs.com)

Schedule
Demo

Arkose Labs bankrupts the business model of fraud. Recognized by Fast Company Fintech Features and Cyber Defense Magazine, 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.

© 2021 Arkose Labs. All rights reserved.