Arkose Labs

THE HIDDEN COSTS OF INEFFECTIVE FRAUD PREVENTION

eBook

INTRODUCTION

Fraud is a multi-billion dollar industry. It's no surprise that so many turn to it to make money quickly rather than pursuing legitimate work. Since the potential payoff is so high, fraudsters will work long and hard to successfully launch attacks against businesses. In fact, fraud costs businesses $42 billion annually in the U.S. alone.[1] Fraud is also drastically increasing on a daily basis; Arkose Labs recorded twice as many attacks on its network in 2020 than in 2019.

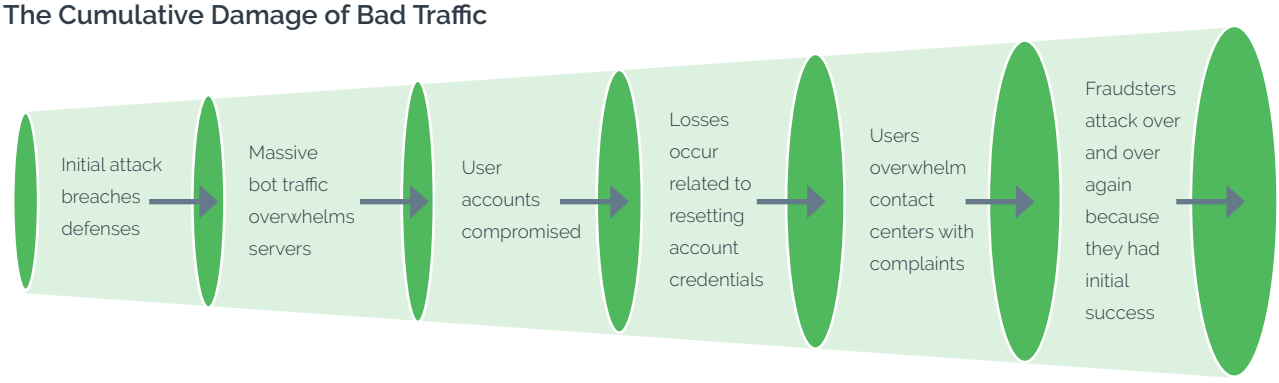
That makes choosing an effective fraud prevention solution of vital importance. The difference between an optimal and ineffective solution can quite literally mean millions of dollars. But what should businesses look for in fraud prevention technology?

PROTECTING THE DIGITAL FRONT-END

The success or failure of an attack lies heavily on whether fraudsters can get into their targeted platform. This is where they spend most of their energy - credential stuffing, brute force attacks, new account origination, and more. Attackers are continuously investing more in their infrastructure and resources to break through businesses' safeguards, which requires smarter investments to protect and detect fraud before it causes downstream damage.

As long as fraudsters can make money from launching attacks, they will continue to do so. We'll explore the full extent of successful fraud attacks and how investing more wisely in early fraud detection can save time and headaches and take money out of the bad actor's hands.

The Cumulative Damage of Bad Traffic



NO SUCH THING AS A FREE LUNCH: THE TRUE COST OF INEFFECTIVE SOLUTIONS

Unfortunately, many companies utilize free -- or nearly free -- fraud solutions that don't provide long-term mitigation against attacks. While going this route is often due to short-term cost considerations, the long-term cost of a solution that doesn't stop repeated attacks is far greater than any initial outlay spent on an anti-fraud platform.

Upfront Cost: The most obvious example of losses associated with the inability to stop fraud is the cost of the initial attack. Resetting passwords for compromised accounts, for example, can cost upwards of $70 per account.[1] The average business loses about 5% of its revenue annually due to fraud; for many companies, this can mean millions of dollars.[2]

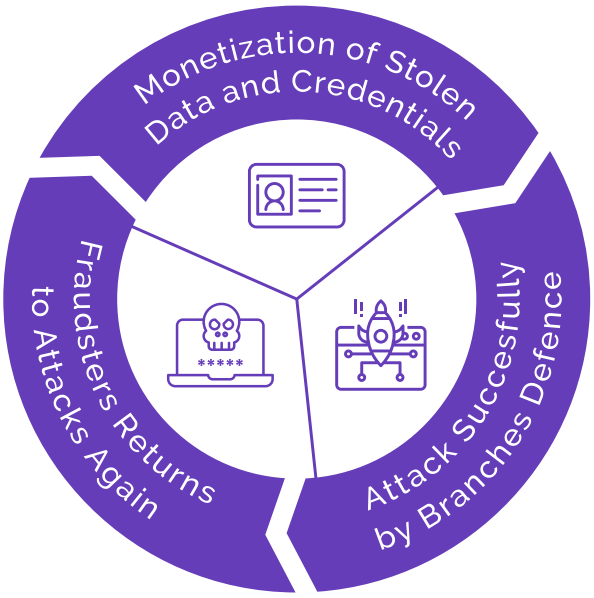
Customer Disruption: Subpar fraud detection solutions have difficulty accurately detecting between good and suspicious traffic. This means too many customers will be blocked or see undue friction, while many bad actors slip through, disrupting online platforms. In fact, in an Arkose Labs poll of 100 fraud and security execs, 90% said successful fraud attacks hinder the user experience.

Negative Branding and PR: A large-scale attack that leads to numerous hacked accounts or disruption to a service or platform will create unwanted negative news headlines and brand association. Customers who are impacted by fraud attacks will also not hesitate to voice their anger on social media and other platforms.

THE ENDLESS CYCLE OF FRAUD ATTACKS

And when a fraudster successfully pulls off an attack against a business, it doesn't end there. If the bad guys know that defenses are easy to breach, they will return time and again.

This leads to a vicious cycle where customer information is exposed, resold and used to commit further fraud attacks. In this way the fraud ecosystem continually fuels itself and attacks grow exponentially. Meanwhile, businesses are constantly putting out fires and dealing with customer complaints and loss of revenue.



THE MONEY PIT: QUANTIFYING CONTINUAL DOWNSTREAM LOSSES

Beyond the initial losses associated with a successful fraud attack against a business, there are many downstream costs as well. Here are just a few examples.

Manual Reviews: When bad actors breach defenses at scale, that means internal fraud teams must take a much more hands-on approach to monitoring traffic. This is time-intensive, costly and requires a lot of manual tuning. In fact, the average business spends between 1-5 hours remediating each ATO attack, according to Arkose Labs polling.

Downstream Customer Disruption: Fraudsters who successfully breach defenses can then use fake new accounts, or compromised user accounts, to send spam and phishing messages to good users, disrupt platforms, manipulate virtual economies and various other types of abuse.

Perpetual Attacks: Fraudsters are not lone wolves; they are part of a robust community that constantly shares information and best practices. That means word will quickly get around if a company has fraud defenses that are easily breached. This means one successful attack will lead to many more down the line.

Operational Costs: A cheaper solution is generally going to be less effective at determining what is good or bad traffic. This affects fraud and security teams who will have to more closely monitor traffic, customer support personnel dealing with compromised accounts and customer acquisition teams.

Increased False Positives: When fraudsters are repeatedly successful in launching attacks, businesses often react by implementing much more stringent controls, including banning accounts and classifying higher percentages of traffic as suspicious. These measures will invariably catch some good users in their net, leading to frustrated customers.

CASE STUDY: MICROSOFT OUTLOOK.COM TACKLES FRAUD AND ABUSE GLOBALLY USING ARKOSE LABS

Cloud-based email platforms are under constant attack from fraudsters looking to create fake email accounts to commit downstream fraud. Attackers use bogus accounts to attempt to blackmail individuals with unfounded threats of revealing compromising information to their contacts. As legacy controls were unable to stop this abuse, Microsoft turned to SMS tokens to stamp out fake new accounts and abuse. Unfortunately, this was an expensive solution that failed to address the problem.

However, after deploying the Arkose Labs platform, Microsoft Outlook.com saw a 33% improvement in good customer throughput. There was a 98% reduction in fraud and abuse, with malicious users being prevented from carrying out large-scale attacks after setting up new accounts. Moving away from SMS verification led to major cost savings. Each check cost significantly less and customer complaints about the SMS verification stopped, relieving the burden on in-house teams dealing with these issues.

THE SOLUTION: A LONG-TERM APPROACH TO FRAUD PREVENTION

To effectively manage fraud and abuse in this rapidly evolving ecosystem, businesses need a long-term approach that evolves with attack patterns, instead of playing a constant game of whack-a-mole with fraud attacks. That's why Arkose Labs takes a different approach; rather than traditional "fraud mitigation" we aim to bankrupt the business model of fraud entirely. By removing the ROI for fraud attacks, fraudsters are compelled to abandon attacking your site and attack someone else.

The Arkose Labs Approach

Eradicates Bots Challenges on the Arkose Labs platform can not be solved by automated scripts, even those using advanced machine vision technology. That's why Arkose Labs offers a 100% bot mitigation SLA.

Frustrates Human Fraudsters When human-driven attacks are detected, they are fed increasingly complex challenges designed to waste their team and abandon the attack.

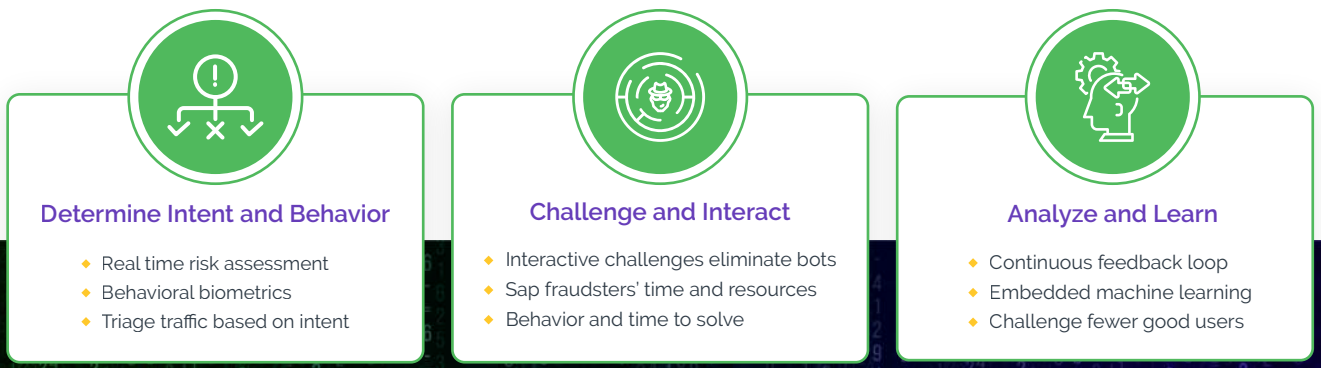
Evolving Platform Utilizing machine learning, the Arkose Labs solution continually adapts to new threats via a constant feedback loop between the custom enforcement challenge and detection engine.

Seamless Customer Experience Good users are never blocked, which eliminates the false positives that hinder customer experience and lead to a negative brand association.

Protect the Entire Digital Front End The platform defends your business against spam, scraping, fake reviews, inventory hoarding, credential testing, fake new account origination, account takeover, bonus abuse, account enumeration and carding.

Managed Services Arkose Labs works with businesses as true partners in fighting fraud, delivering custom insights, scalable defenses for anticipated high-traffic events and 24/7 customer service.

The Ideal Fraud Defense: Detect, Stop and Continually Evolve



CONCLUSION

Fraudsters get up every morning and do a job, just like anyone else. The antiquated image of a fraudster sitting in a dark basement wearing a hoodie is no longer the truth, if it ever was. These are people who launch attacks carefully and methodically and calculate their return on investment beforehand.

They continue to pursue this line of work because it pays for them, often more so than a "regular" job might. The only truly effective way to stop the scourge of online fraud and abuse is by making it uneconomical for fraudsters to engage in this line of work. If they can't make money in it, they will simply stop.

That's why it is imperative for businesses to deploy a fraud solution that stops attacks at the digital front door. By doing so, fraudsters will be unable to make money from the myriad of downstream abuse they engage in after initially breaching a business's defenses. By bankrupting the business model of fraud, businesses can stop attacks before they even begin.

Arkose Labs

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.

Sales:

(800) 604-3319

Mail:

support@arkoselabs.com

Address:

USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006

Schedule Demo