Aite PARTNER. ADVISOR. CATALYST.

IMPACT BRIEF

MAY 2021

David Mattei
+1.617.398.0908
dmattei@aitegroup.com

Arkose Labs Case Studies: Stopping Fraud by Making Attacks Too Expensive

This report provided compliments of:

As consumers have moved online, the fraudsters have followed. Digital accounts are under attack like never before. With the proliferation of data breaches, fraudsters have access to billions of records of personally identifiable information, including usernames and passwords. With that level of scale, it is impractical to conduct attacks manually. Fraudsters have created bots (short for "robots"), which are computer programs that automate these attacks, thus creating a higher level of efficiency. They are pointing these bots at online accounts consumers have at financial institutions, social media, and merchants to gain unauthorized access and commit their crimes.

This case study examines how three companies are protecting themselves and their customers from this form of fraud using solutions from Arkose Labs.

HUMAN AND AUTOMATED FRAUD ATTACKS

It is easier than ever for fraudsters to commit their crimes. With billions of compromised personal information and credentials, low-cost and free tools to commit attacks, and a growing knowledge of weaknesses in defenses, fraudsters are using a combination of bots and human farms to deploy sophisticated and persistent attacks. They are creating fake online accounts and taking over existing accounts to gain entry for their nefarious intents. Examples are listed in Table A.

Table A: Examples of Fraudulent Attacks

Type	Description
Account takeover	Using a treasure trove of username/password combinations from data breaches, fraudsters use bots to test these combinations and find valid ones. Since passwords are commonly reused, there is a good chance the combination will work on an e-commerce or banking application.
New account origination	Creating online accounts can be manually intensive for fraudsters due to the amount of data entry required to perform this task. Fraudsters use automated bots to create new online accounts that can be done at scale.
Human fraud farms	An online account login may prompt a user to perform a manual task that the bot may not have the ability to do. In these situations, fraudsters employ people to perform the task to gain access to the account. This combination of automation plus humans is difficult to stop.
Puzzle solvers	To prevent automated attacks, some websites deploy a captcha puzzle, involving deciphering a text string or a set of pictures. Once the puzzle is solved, the user gains access to the account. Some automated bots are sophisticated enough to solve the puzzle without human intervention.

Source: Aite Group

Not all attacks are fraudulent in nature. Other abuse targets customer touch points that can be monetized to take advantage of the target company or to disrupt legitimate ecosystems companies establish with which their users interact. These types of attacks cause customer dissatisfaction issues and damage the reputation of the targeted company and lead to indirect losses for the business. Examples are listed in Table B.

Table B: Examples of Malicious Bot Tactics

Type	Description
Online auctions	For desirable products that have a high resale value, these bots will outbid a legitimate person within seconds of an auction closing, allowing the party to make a profit on the difference between the auction price paid and the resale price or by gaining possession of a physical or digital asset.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Type	Description
Inventory hoarding	Common with online ticket sales to entertainment events, bots will rapidly buy goods that are resold on the secondary market at a higher price, preventing individuals from purchasing on the primary market.
Loyalty/promo abuse	To attract enrollment in loyalty programs, companies may offer an incentive to new members (free product, coupon code discount on future purchases, etc.). Bots will create rapid, successive loyalty accounts to acquire the incentive, which is then resold.
Web scraping	Malicious web scraping can extract a variety of data from websites, including price scraping where competitor websites are scanned to ascertain product pricing used to help a company to undercut them in price.

Source: Aite Group

Companies have deployed various defenses such as traditional bot detection at the network layer to block high-risk internet traffic as well as captcha puzzles at the application layer to separate bad bots from good bots and bots from humans. Fraudsters leverage a combination of machine learning (ML) technology and human fraud farms to circumvent these defenses. Companies have also indiscriminately deployed captcha puzzles requiring all website visitors to solve them resulting in a poor experience for legitimate users.

Due to this vexing problem, Aite Group spoke with three companies that have deployed the Arkose Labs fraud and abuse prevention solution to address this. Two companies are international entertainment companies and the other is a financial services firm.

ARKOSE LABS OVERVIEW

Arkose Labs was founded in 2017 by Kevin Gosschalk, who recognized an opportunity to disrupt fraudsters by sabotaging their economic model and make it more costly to commit their attacks.

They developed a platform that combines risk-based decisioning with adaptive friction. The platform assesses the risk of digital traffic in real time using device, network, and behavior intelligence. This risk classification informs the platform of any secondary screening that is required for suspicious traffic, while good users are able to pass through seamlessly. Bots are met with anti-automation challenges, which are tested against advanced ML tactics to ensure they cannot be solved at scale. Malicious humans are presented with challenges that are increasingly time consuming to solve in order to frustrate their attempts to attack at scale.

Their approach is designed to provide robust protection while preserving the online experience for legitimate consumers. The vast majority of good users (95% or more) never see a challenge. In the event they do, challenges are simple to solve and provide an option to self-remediate, rather than blocking suspicious activity or damaging the user experience with difficult challenges or by sending users out-of-band authentication.

This combats large-scale fraud and abuse attacks by causing bots to fail and wasting fraudsters' time and resources. This drives up the costs of attacking, compelling fraudsters to abandon attacks and move on to softer targets. The Arkose Labs platform has three components:

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Arkose Detect, which classifies web traffic into good, suspicious, or bad categories
- Arkose Enforce, which adds adaptive friction to bad actors using a type of varying puzzles that are easy for good users to solve but difficult for bots and fraud farms, deterring future attacks due to the high cost
- Arkose Global Network, which shares anonymized fraud intelligence and emerging attack patterns across all customers on the platform

Arkose Labs protects against many forms of abuse including:

- Account takeovers
- New account origination
- Credential stuffing
- Spam and malicious content
- Web scraping
- Payment fraud
- API abuse

The solution sits at the application layer, such as the login page, which more sophisticated bots are able to reach. This is different from traditional bot solutions, which are deployed at the firewall layer and are primarily focused to prevent distributed denial of service (DDoS) attacks. Since the solution is application based, a company can customize the installation of Arkose Detect and Arkose Enforce for each of its applications.

The company name pays homage to Kevin Gosschalk's homeland, where there is a type of rock called arkose in the middle of Australia. If one is starting an anti-fraud company, naming it after something as strong as a rock would be a good thing.

BACKGROUND/HISTORY: DIGITAL GAMING FIRM

This merchant is a significant player in the digital gaming industry that was using a legacy bot detection solution. The legacy vendor changed its business paradigm and moved from a free version to a paid version. This provided the digital gaming firm with the impetus to research other fraud solutions to see if there was a better one that met its needs. In addition to finding a more feature-rich solution, the digital gaming firm was able to expand its geographical footprint with support of additional countries with Arkose Labs.

APPROACH

The digital gaming firm found it was a good time to consider a new solution because its legacy vendor would have required a reinstallation of the solution. Moving to the more feature-rich solution of Arkose Labs was a no-brainer since the effort to deploy it would be about the same.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

The implementation took approximately two to three months and has been in production for one month.

The digital gaming firm is very enthusiastic about its partnership with Arkose Labs. The firm rated Arkose Labs very high on its responsiveness to questions arising during the implementation phase, giving the company a score of 5 out of 5. Even when questions came up "at all times of the day and night," it promptly received responses. The firm also rated customer service as "amazingly good."

It was a collaborative effort to get the solution installed and configured, involving tweaks and changes by Arkose Labs and the firm. Almost immediately, the firm's team noticed fraudsters pivoting in an attempt to circumvent the Arkose Labs solution. With this feedback, Arkose Labs and the firm worked together to manage day-to-day activity, continually fine-tuning the solution and keeping fraudsters out. Once steady state is achieved, it expects the need for ongoing tweaks to subside.

OUTCOMES

Early results from the digital gaming firm's deployment have had a positive impact in the following three areas (Table C).

Table C: Digital Gaming Firm Benefits With Arkose Labs

User experience	The prior solution added more friction to good customers than was needed, and the captcha puzzles could be difficult to solve. The firm was happy to see an increase in the ability for a good customer to solve the puzzle, creating a positive improvement in user experience over the legacy solution.
Customer support	The digital gaming firm has multiple types of fraud solutions deployed in its environment to address multiple attack vectors. Of all the vendors it does business with, it rates Arkose Labs highest in customer support and responsiveness. As an example, in a demo to senior management, one of the managers commented about the name of a field on the dashboard that he did not like. While somewhat trivial in scope of the overall solution, Arkose Labs was able to rename the field within 30 minutes, which really impressed the senior manager.
Customization	Customized branding has helped the firm improve its customer experience. The digital gaming firm was able to provide Arkose Labs custom graphics that were used to create puzzles that provided customers a more personalized experience. The firm did not have to make any changes to its implementation for the new puzzle graphics to be deployed in production.

Source: Digital gaming firm

In a sign of the partnership that has been fostered with Arkose Labs, the firm stated, "You want a vendor to feel invested in your success, and that is how we feel about them."

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

LOOKING AHEAD

In just one month of production usage, the digital gaming firm has seen value from the out-of-the-box solution. Although some customization and fine-tuning are needed to meet its unique needs, the firm has found the system easy to tune.

The digital gaming firm takes a layered approach to protecting itself against fraudsters. Arkose Labs was a welcome addition to its fraud stack, which also includes risk-based authentication on logins, device ID and behavioral biometrics, and an in-house, ML-based risk engine used on purchases. It also deploys bot detection on the edge of its network to provide API protection and prevent DDoS attacks. The digital gaming firm believes that over time, there will be opportunities to sunset some of these fraud tools based on Arkose Labs' performance.

BACKGROUND/HISTORY: DIGITAL BANK

This client is a financial services firm that operates online; it does not have physical branch locations. A new executive came on board, examined its fraud protection system, and determined a new approach was needed. Having kept an eye on innovative industry solutions, the executive recalled Arkose Labs and decided to deploy it.

APPROACH

The digital bank started its implementation with the web channel and has plans to expand the solution to its mobile banking and then mobile API. The partnership started strong; in the three months to implement the solution, the digital bank's engineering team has been "incredibly impressed with the responsiveness of Arkose." Weekly calls have been established with email interactions as needed. Questions are answered in minutes, not days. The engineering teams across the two companies have built such strong relationships through the implementation that they socialize outside of work. The digital bank says this is a testament to "how well and how closely the two teams are working and appreciate each other."

Arkose Labs is not a "set it and forget it" type of solution. Those types of fraud systems don't tend to perform well over time since fraud is dynamic and the fraudsters are always finding new attack vectors. Even after the bank achieves a steady-state operating model, it expects some low-level tuning will always be needed. The internal fraud team looks at what fraud gets through and adjusts its system (rules, thresholds, etc.), while the Arkose Labs support team continually trains the platform based upon observed behavior and bank feedback.

OUTCOMES

There have been several benefits the digital bank has achieved since deploying Arkose Labs, as noted in Table D.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table D: Digital Bank Benefits From Deploying Arkose Labs

Benefit	Description
Reduction in fraudulent logins	On its initial launch, the digital bank saw a significant rise in users abandoning their login. It attributes this to automated bot activity not capable of circumventing the Arkose Labs solution.
Lower user friction	Only high-risk users, as defined by Arkose Labs and its ML model, are prompted to solve a puzzle. For example, with the prior system, a customer changing devices would be considered high risk, resulting in a challenge, or worse, outright decline. Arkose Labs risk engine looks at other attributes of the login attempt, identifies that it is an existing good customer, and can be configured to either not require a challenge (eliminate friction) or at least provide a challenge puzzle to solve (allowing a good customer a path to gain access to their account) instead of a hard decline.
Customization	Financial institutions, merchants, and other digital platforms have varying levels of sensitivities when it comes to fraud and user challenges. In situations like banking, friction may be viewed as a higher level of security and appreciated by the user, whereas in other cases, it may be frowned upon. The digital bank likes how Arkose Labs' solution can be configured and how high-risk thresholds can be set differently across its customer base.
Lower false positives	Turning away good customers because you think they are fraudsters leads to high dissatisfaction. The executive interviewed likes the Arkose Labs feature of prompting the user to self-remediate. Other solutions would block too many good customers; they didn't provide an option for the customers to prove they were legitimate and do a hard decline. Arkose Labs allows customers to solve a puzzle and continue the login since good customers solve puzzles differently from fraudsters.

Source: Digital bank client

The digital bank has been pleased to see quick reductions in its fraud losses even in the early stages of deployment, which is a great sign of what's to come.

LOOKING AHEAD

The digital bank is investing in a data science team and a data lake. Therefore, collecting as many risk signals as possible is important to the bank executive. The executive is investigating using Arkose Labs APIs to feed additional risk signals from the platform into its ML model for transaction decisioning. A solution provider that returns only a fraud score has limited value. This executive likes the additional raw data feeds from Arkose Labs, which include user-specific login volume, device and behavioral signals, and others. Eventually, the bank hopes to sunset its legacy solution, which would simplify the environment and lower costs.

Many vendor implementations require involvement from the customer's engineering team. It is common that progress cannot be made as fast as one would like. This bank's implementation will be around three months, which many would consider to be quite short compared to the time

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

required for other solutions. The three-month implementation is more of a factor of the bank's engineering team and not a reflection of Arkose Labs, which has been responsive.

BACKGROUND/HISTORY: VIDEO ENTERTAINMENT FIRM

This client is a video gaming company with a large presence in North America and Europe. It faced an unusual situation in which the problem was not traditional fraudsters but malicious activity from users within its ecosystem. With some of the games, players can trade digital game assets via online auctions. Some players were using bots to outbid other players by submitting a winning bid within a few seconds of an auction closing, preventing other players the ability to acquire desired digital game assets. This was leading to customer dissatisfaction.

APPROACH

The video entertainment firm has a team responsible for one specific game with high rates of bots outbidding other players. The team began a search for solutions to separate people from bots. In that search, they found Arkose Labs, which provided several attractive benefits, as noted in Table E.

Table E: Video Entertainment Firm Benefits Using Arkose Labs

Feature	Benefit
Ease of integration	Some bot solutions at the network layer can be invasive to deploy requiring considerable integration effort. Arkose Labs was "super simple" to deploy.
Managed services	Advanced fraudsters deploy ML to solve captcha puzzles. The Arkose Labs detection engine monitors for this, while its team of security experts tune the system to allow people through and keep bots out. This alleviates work for the client.
Puzzle customization	Since the video entertainment firm is in the gaming business, solving an interactive puzzle fits well with its client base. With challenges customized with its branding, the firm maintains the integrity of its gaming experience as compared to using one-time passcodes or other means of stepped-up authentication.

Source: Video entertainment firm

The deployment was simple; all the client needed to do was modify a web page and republish it. The firm configured its implementation to allow it to manage the overall user experience. When a user shows interest in making a purchase or bid in an auction, Arkose Labs is invoked. Once the user initiates a transaction, the video entertainment firm makes a call to Arkose Labs to retrieve the results of its analysis of the user. The client has built an ML model to determine what action to take on the transaction. The Arkose Labs results, along with other data the merchant has, is fed into its model. Based on the outcome of the model, it will determine what action to take: approve, suspend the account, slow down fulfillment, deny the transaction, or others. The client appreciates the flexibility in how the Arkose Labs platform can be configured.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

OUTCOMES

The video entertainment firm has been using Arkose Labs for four years and has found the solution to be very effective at lowering fraud. When the original team went live with Arkose Labs, they saw "fraud drop through the floor." Migration from proof of concept to production occurred quickly based on the results.

Fraudsters are dynamic and are always looking for new ways to circumvent defenses. Arkose Labs continuously monitors many aspects of the puzzles that are solved, dynamically adjusting them to weed out the fraudster. The client leverages built-in dashboards to see ML scores produced by Arkose Labs' model, traffic analysis, and actions taken to mitigate bad behavior, which are helpful to monitor the system and ensure it is operating properly.

Since the video entertainment firm use case is unique, it appreciates how Arkose Labs customizes its ML system for its needs. It can also send Arkose Labs feedback on false positives, which is fed back into the model for learning purposes. This alleviates the need for the video entertainment firm to staff ML engineers to maintain this aspect of the system.

The Arkose Labs' implementation has lowered friction for good customers since not all users are prompted to solve an interactive puzzle. The video entertainment firm was able to define what kind of challenge experience it wanted users to have, and Arkose Labs tuned the system accordingly. For example, the client stated it did not want to challenge a heavy user more than once per week, and Arkose Labs configured its system to perform that way. Over time, it can adapt, improve results, and challenge less.

LOOKING AHEAD

Arkose Labs is one of several solutions the video entertainment firm has running in production. Other tools include an anti-cheat solution (unique to gaming), device fingerprinting, payment fraud for card transactions, and others. Given the success seen to date, the video entertainment firm is exploring other use cases Arkose Labs can address, such as account creation, account takeover, and replacing one-time passcodes. It would like to see Arkose Labs explore other potential use cases based on the breadth of data it collects. This could potentially allow it to sunset some solutions in production and reduce the number of vendors with which it interfaces. IP address reputation is one potential example.

CONCLUSION

Fraudsters continue to evolve over time and as the sophistication of their attacks grows. Stopping fraudsters and undesirable user behavior is a never-ending war to wage. Based on interviews with these merchants and bank, companies should consider the following:

- The goal should not be to eliminate all user friction. Rather, the focus should be on risk-based friction. Apply it when necessary, and allow good customers an opportunity to gain access to their accounts (via solving a user challenge), rather than experiencing a hard decline.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Needs and requirements vary across companies and industries. Ensure your solution providers can customize their system to meet your needs since it is rare for an out-of-the-box solution to meet your needs all the time.
- No single solution will solve all your fraud prevention needs. But a robust, multifaceted solution that provides protection across multiple use cases can reduce the number of vendors you need, which is a cost savings and efficiency play in the long term.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

RELATED AITE GROUP RESEARCH

Managing Lending Fraud: Digital Identity and Machine Learning Are Table Stakes, February 2021.

Revisiting Your Authentication Control Framework, December 2020.

Application Fraud: Accelerating Attacks and Compelling Investment Opportunities, November 2020.

The Digital Channel Under Attack: How to Protect Yourself and Your Customers, June 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com