Arkose Labs

THE ULTIMATE GUIDE TO NEW ACCOUNT FRAUD

EBOOK

INTRODUCTION

In today's highly competitive digital economy, organizations are under relentless pressure to acquire new customers and accelerate growth. Attracting and retaining loyal customers requires rolling out the virtual red carpet from the outset. Therefore, the account opening process has become a make-or-break customer touchpoint for ongoing commercial success.

Offering a seamless registration process requires demanding minimal information from the customer at the outset, which makes it increasingly difficult to determine if a customer signing up for a new account is who they say they are. Digital identities have been compromised en masse, with fraudsters exploiting the wealth of stolen identity data, alongside a wide range of freely available tools and technologies used to attack businesses with great effect.

It's no surprise then that the account registration process has consistently been the most attacked customer touchpoint on the Arkose Labs network. Businesses offering freemium models and bonuses for new customers are particularly at risk from direct abuse at the account opening stage - however, all businesses must be vigilant. Creating a seamless sign-up process while also being vigilant about protecting against fraud can be a difficult tightrope to walk.

NEW ACCOUNT FRAUD: A PANORAMA OF ABUSE

Fraudsters have devised many inventive ways to monetize fake new account registrations. These range from high-scale, bot-driven identity credential testing to low-scale, more targeted attacks. While the higher-volume attacks will be primarily driven by automation, fraudsters are also turning to low-cost human resources in so-called "sweatshops" to carry out more nuanced attacks at scale. As a result, organizations need active protection against both human-driven and automated attempts across the spectrum of abuse use cases.

Fraudulent Applications: An example of these types of attacks are when fraudsters use stolen credentials to sign up for new accounts, such as signing up to take out a loan with a fintech lender that the fraudster has no intention of paying back or applying for a new credit card.

Promo Abuse at Scale: Large-scale abuse of new customer promotions falls under this category. These can range from fraudsters exploiting and selling free trials, gaining access to new products or introductory cash discounts or credits. This is usually carried out at scale using scripts or human sweatshops and can be a quick revenue source for the bad actors.

Synthetic Identity Farming: In a digital world, identities are the real currency and synthetic identities are really covered items in the fraud ecosystem. This is where fraudsters create fake identities and establish credit profiles by using real data stolen from a number of different individuals to create a composite identity that appears real.

Account Validation Attacks: Fraudsters often use a new account origination process to test the validity and existence of an account or payment credential before launching organized account takeover or payment fraud attacks.

Affiliate Fraud: In this category fraudsters create fake accounts to take advantage of affiliate marketing programs at scale, thus abusing a legitimate business practice to get companies to pay them. Bots are most often deployed to commit affiliate fraud at scale.

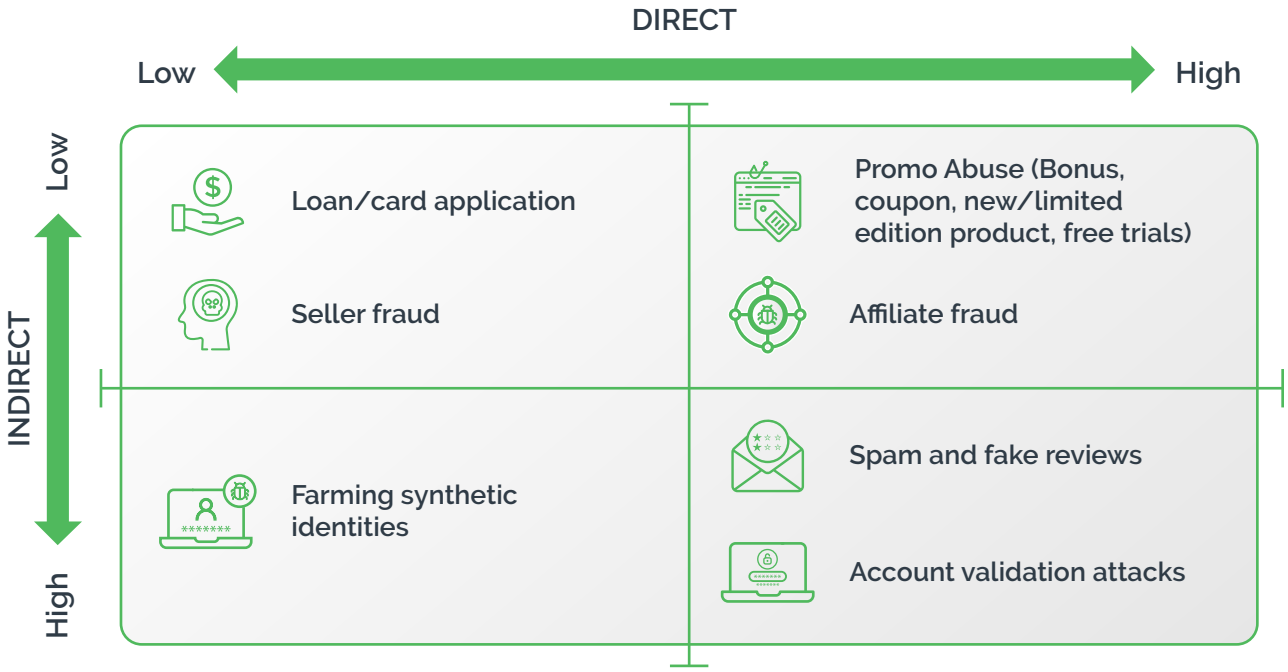
Spam Abuse: Fraudsters often create new accounts at scale in order to write fake reviews or send spam and phishing messages with platforms, such as social media or dating services.

MULTIPLE PATHS TO MONETIZATION

In recent years, there has been a strong trend towards more complex, orchestrated attacks wherein fraudsters focus on multi-step attacks that hide their true malicious intent from the outset. This plays out at the account registration stage, where attacks range from those that inflict direct losses on the business in question, to less direct attacks which are laying the groundwork for downstream fraud.

The potential direct and indirect losses and the implications for the wider digital ecosystem are why it is imperative to stop account origination fraud at the front door. In the end, it's the business and legitimate customers who are the ones that suffer.

New Account Fraud Monetization Grid



SPOTLIGHT: THE MANY FACES OF BONUS ABUSE

As competition for the consumer dollar heats up, many businesses rely on bonuses or special promotions to entice new customers. These, however, are also prime targets for fraud due to the high monetization potential.

Examples Across Industries

Bonus Abuse in Online Gambling and Betting: Online betting and gambling operators often offer sign-on bonuses as a way to entice new customers. Fraudsters sign up en masse to either collect these bonuses, run a collusive play, dump chips or increase their willing chances through arbitrage by placing multiple bets using the bonus.

New Product and Promo Abuse in Online Gaming: As online gaming has exploded in popularity so have "microtransactions" within games. These are typically item upgrades, character power-ups or new "skins" that players can purchase for a small fee. As a way to entice new customers, many online gaming platforms offer one of these types of items for new users. Fraudsters create new accounts en masse and re-sell these digital goodies for real money to gamers on gaming auction platforms.

New User Bonus in Tech Platforms: Many tech platforms offer sign-up bonuses to customers that can be redeemed against future usage. Fraudsters often abuse these promotions by creating accounts at scale and using the bonus to use the platform as an enabler to downstream fraud.

Streaming Service Free Trial Abuse: The explosion in video streaming services, and associated costs with each, have led to many people looking at creative ways to get them for free. This can range from a fraudster avoiding paying for the services by continually signing up for the free trials using different accounts to an organized fraud operation to re-sell these "subscriptions" at a discounted rate in other regions.

Coupon Fraud in Retail: There are numerous ways that professional fraudsters and regular consumers alike can abuse coupons. These include so-called "decoding" wherein the coupon is used for an item or service beyond what was originally intended, counterfeiting and making multiple copies of coupons or reselling coupons. This type of fraud is on the rise, coupon abuse rose 10% in 2019, and costs businesses billions annually.

Referral Bonus in Fintech: This is another customer acquisition tactic that is frequently abused by fraudsters. Take this scenario common with robo advisor firms: many offer a free share of stock in a random company for every friend a user refers that becomes a customer. Fraudsters create large quantities of fake new accounts as a method to gain stock shares in companies without having to spend any money.

Laundering Stolen Money in Online Gambling: Fraudsters also use online gambling sites to collude with one another by sitting on the same table and one player purposely losing to another repeatedly to effectively launder money using the platform. Digital, peer-to-peer payments apps -- that typically offer instant sending and receiving of funds -- are also used for this purpose.

Limited Edition Items in Speciality Retail: Retailers often use limited-edition items to drive customer loyalty. A sneaker company may offer customers who have downloaded their app and signed up for a rewards program the first crack at a limited edition shoe. Fraudsters use this opportunity, via bots or sweatshops, using multiple accounts to acquire a large number of limited items. These can then be re-sold for a massive profit.

CASE STUDY : ARKOSE LABS HELPS A CLOUD COMMUNICATIONS PLATFORM STOP BONUS ABUSE

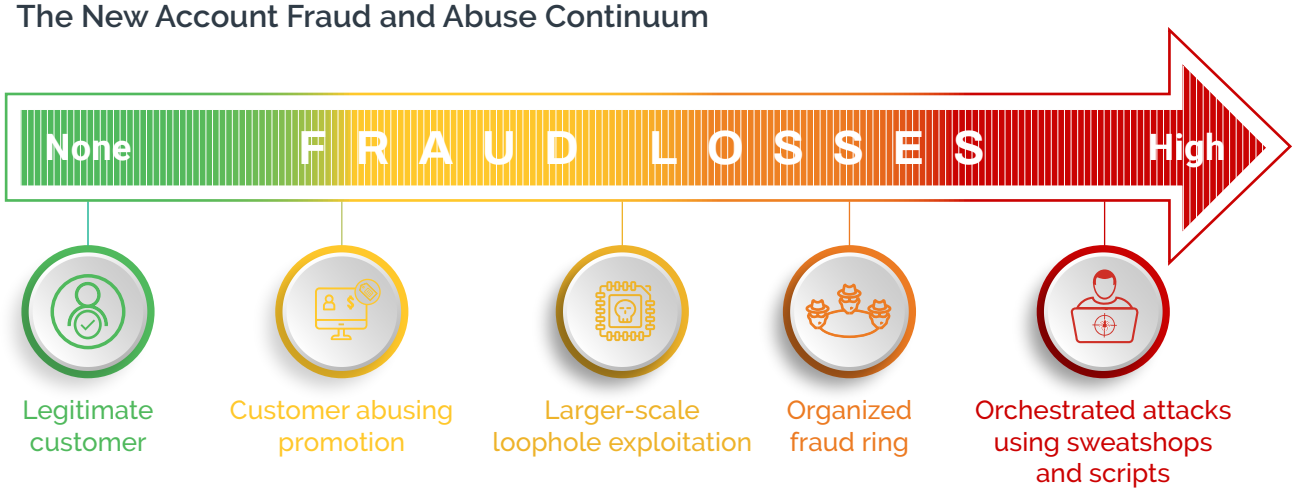
Overview: This company enables software developers to use its APIs to programmatically make/send and receive phone calls/text messages, and perform other communication functions. The company was offering a new user promotion in the form of phone credits that fraudsters were abusing to call premium numbers and commit downstream fraud. They needed an effective way to stop these fraudulent new accounts that were leading to losses and customer complaints.

Arkose Labs Solution: Using the Arkose Labs platform the company was able to identify suspicious traffic and use adaptive step-up challenges to sap the fraudsters' efficiency in creating fake accounts without impacting good user experience.

Demonstrated Results

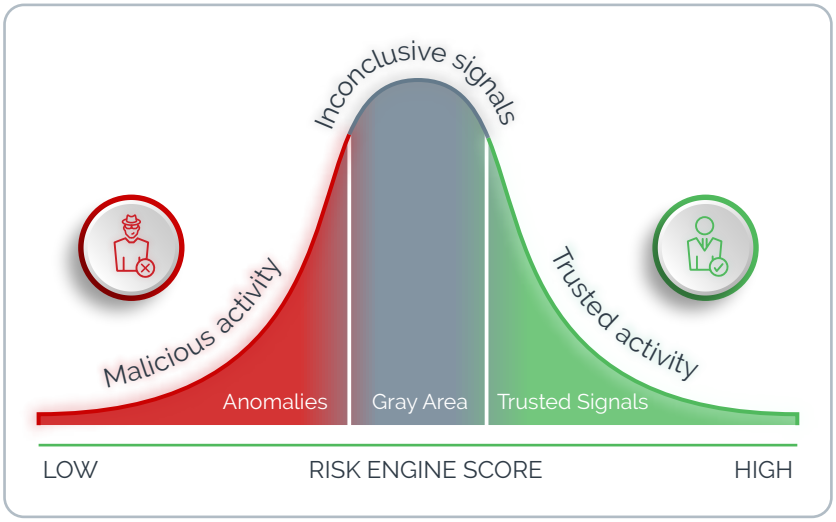
Eliminated fraudulent new account originations and prevented downstream fraud and abuse

The New Account Fraud and Abuse Continuum



OVERCOMING THE LIMITATIONS OF TRADITIONAL METHODS

Fraudsters are constantly refining their ability to bypass standard fraud detection systems, and widely adopted solutions can quickly become obsolete.



Genuine customers' behavior is increasingly unpredictable, whereas bad actors continually get more sophisticated in spoofing and cloaking techniques using stolen data. While there are sometimes clear identifiers that mark out traffic as clearly "good" or "bad", an increasing amount falls under a gray area in between. As such, data-driven decisioning tools that rely on extreme signals are unable to deal with inconclusive signals.

Unfortunately, data alone cannot be trusted. Scores of data breaches mean that nearly anyone's personal information is available for purchase on the Dark Web. And, as discussed above, cybercriminals have a plethora of tools at their disposal that can mask their digital footprint. One doesn't even need to be an expert to carry out these attacks, video tutorials and even customer support services are available to the enterprising fraudster. That's why traditional authentication techniques are largely ineffective today.

Here is a quick look at some traditional methods and their limitations:

SMS Tokens: SMS codes, while widely used, are ineffective at stopping fraud as they can be easily hijacked, impact good customer experience and are expensive to send -- usually about 3 cents per instance. They are especially ineffective in verifying new account origination fraud and add high friction for good users without impacting the fraudsters. The experience associated with SMS is disjointed as the customer is taken out of the sign-up flow causing abandonment. SMS messages also

often get delayed or sometimes don't get delivered if they get caught in range blocks associated with areas where scammers usually operate or if the phone number is VOIP. On the other hand, the impact on the fraudsters is minimal as they can automate the process, don't care about user experience and are willing to put in the effort and resources to carry out the fraud. For a fraudster, the downstream monetization potential of a successful account origination (fake loan, promo abuse, spam/fake reviews) far outweighs any costs associated with getting a new number and receiving an SMS. In the end, the fact SMS codes are easily corruptible, combined with the annoyance they cause to good customers while having minimal impact on fraud prevention, means they are simply not worth the effort.

Data Intelligence: Anyone looking to commit fraud can easily find software online that allows them to manipulate data signals, such as their device, IP address or location in order to bypass the signals that traditional risk management solutions look for. At the same time, businesses can't just assume everyone using these tools have bad intent; many good users who are vigilant about privacy concerns sometimes use tools to mask their digital presence. Therefore, solely relying on data insights is not enough.

Bot Detection: Fraudsters are increasingly turning to low-cost human resources to scale up attacks, and launch hybrid attacks that use a blend of automation and human activity. Point solutions focused on bot detection struggle to defend against more sophisticated attacks, low-and-slow bots, and human sweatshop activity.

Legacy Visual Challenges: Legacy visual challenges can easily be bypassed using commercially available software while the completion rates for good users can be as low as 65-70%. This offers a bad experience for customers who have had their fill of clicking on crosswalks and traffic lights but are vulnerable to being solved at scale by automated solvers using machine vision technology or being farmed out to low-cost sweatshops.

CASE STUDY: LARGE TECHNOLOGY PLATFORM UPLIFTS CUSTOMER THROUGHPUT AND REDUCES FRAUD BY DEPRECATING SMS

Overview: This global technology giant was under constant attack from fraudsters creating fake email accounts to send spam and malicious content as well as commit downstream fraud. Their existing SMS based solution had severe limitations as fraudsters were able to automate around it. Meanwhile, it was disrupting true users' experience and cost the company a fortune. The company needed an effective solution to stop fraudulent new account creations, reduce spam and abuse, and improve customer throughput in a cost-effective manner.

Arkose Labs Solution: The company deployed Arkose Labs to differentiate between good customers and eliminate spam and abuse. New users were shown enforcement challenges prior to their first email and the company implemented custom rules and policies to detect suspicious behavior downstream. Adaptive step-up challenges sapped the fraudsters' efficiency, eliminated mass dissemination of malicious emails while preserving a good user experience for genuine customers.

Demonstrated Results
With Arkose Labs, the company saw a 33% improvement in good customer throughput along with a 98% reduction in fraud and abuse. This also stopped customer complaints about SMS verification.

Knowledge-Based Authentication (KBA): The easy availability of personal data, as well as using tactics like social engineering, means that KBA's are easy for fraudsters to solve. In fact, studies show bad actors pass KBA methods at higher rates than good customers do, who often can't remember the name of their first dog or best friend in 1st grade.

A NEW APPROACH: BREAKING THE BUSINESS MODEL OF FRAUD

Fraud levels will continue to rise indefinitely unless businesses stop tolerating fraud as a 'cost of doing business.' Allowing for a certain level of fraud actively feeds the cybercrime cycle of success, enabling fraudsters to continually improve their ability to launch and expand successful attacks. Instead, the focus should be on disrupting fraud so that it ceases to be a lucrative option for cybercriminals, no matter where they are in the globe. This requires targeted action that increases the costs involved for fraudsters to launch attacks, increases the strain on the resources required to carry out attacks, and shifts the attack surface.

But just as important as slowing down fraudsters is, it is equally important that returning good users are not continually seeing a high level of friction. If, for example, a new user with a never-seen-before device or IP address arrives at a businesses site to register as a new user, they will be asked to complete a simple challenge in order to proceed. But as that person builds more of a digital footprint and demonstrates signs of "good" behavior, they will not see any further friction on each return to the site. False positives have a damaging effect on both consumer trust towards a business as well as the bottom line. It is imperative that good users do not become collateral damage in the fight against fraud.

ARKOSE LABS FRAUD AND ABUSE PREVENTION PLATFORM

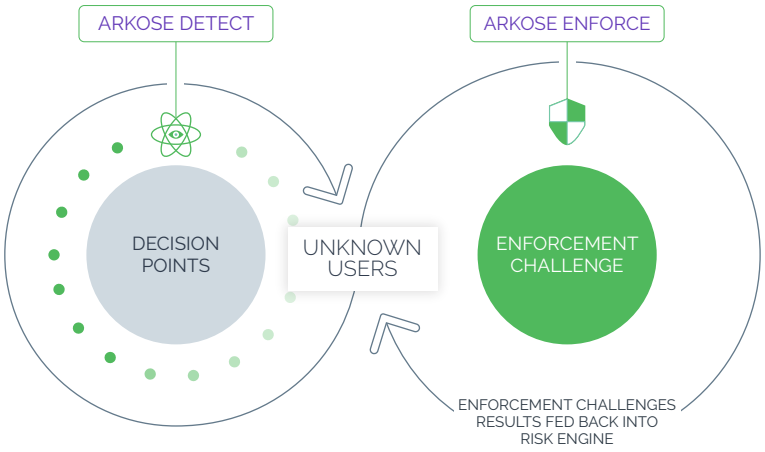
The Arkose Labs Fraud and Abuse Prevention Platform combines real-time intelligence, rich analytics, and sophisticated step-up challenges to progressively diminish the profitability of attacks while adapting to evolving attack patterns. There are two distinct components of the platform:

Arkose Detect

Arkose Detect is a dynamic risk engine that analyzes data from user sessions and their interactions with technology. It unearths behavioral patterns across devices and networks in real-time. Combining this data with behavioral patterns, Arkose Detect accurately triages traffic based on the risk profile, informing any secondary screening required by Arkose Enforce.

Arkose Enforce

Arkose Enforce delivers adaptive enforcement challenges that accurately distinguish between authentic users, malicious humans, and bots, thereby protecting against online abuse and fraud. The challenges gradually increase in difficulty depending on the associated risk of the user. This increases the time required for fraudsters and wastes their resources when trying to clear challenges at scale. Since increasing costs diminish the profitability of the attacks, fraudsters are compelled to stop.



THE ARKOSE ADVANTAGE

- Eliminates 100% of automated attacks
- Protects against even the most sophisticated forms of fraud
- Authentication built with user experience at its core
- Challenges commensurate with the risk profile of each user
- Advanced data analysis can spot even the subtlest for of fraud
- Continually updated platform with continuous feedback loop between risk engine and enforcement
- Saps human fraudster's time and resources
- Serves as critical buffer between the business and attackers
- Easy implementation that does not require major IT work

When new users are signing up online, a business often has limited context or information with which to assess their legitimacy. Arkose Detect delivers protection based on previous attack patterns, data identifiers and telltales and shared intelligence to provide insights into the underlying intent of a new user. Arkose Enforce acts as a sandbox for suspicious traffic and provides the ability for a secondary screening. While genuine users can easily clear the challenges, suspicious traffic is presented with incrementally complex challenges that demand time and extra resources to complete. This permanently disrupts the economic viability of organized attacks and breaks the fraud model to stop both human and bot-driven attacks.

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