Arkose Labs

Ebook

The High Cost of New Account Fraud

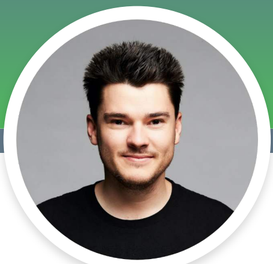
A Data-Driven Report From Arkose Labs

The High Cost of New Account Fraud

New account origination (NAO) fraud is one of the biggest issues facing businesses today. Fraudsters use fake new accounts for a variety of different attacks, including creating a fake profile on a dating app with the intention of sending phishing messages; setting up bogus online gaming accounts to accrue in-game assets using bots; or setting up financial accounts in other people's names to get credit. New account creation fraud powers a wide range of downstream fraud attacks, which is why it is so important to stop it before it happens and causes problems for businesses and users.

New account registration attacks can be monetized in many different ways depending on the industry and account type. Attacks range from those that inflict direct losses on the business that was attacked, 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.

To find out how businesses are dealing with new account fraud, Arkose Labs commissioned a survey of 100 IT executives, in conjunction with market research firm Pulse, across a range of industries and geographies on a number of topics related to this specific type of fraud. It's clear from the results that NAO fraud is a major burden on digital businesses that affects the user experience and hurts the bottom line. By stopping fake new account fraud before it happens, many attacks can be rooted out before they do any harm.



Kevin Gosschalk

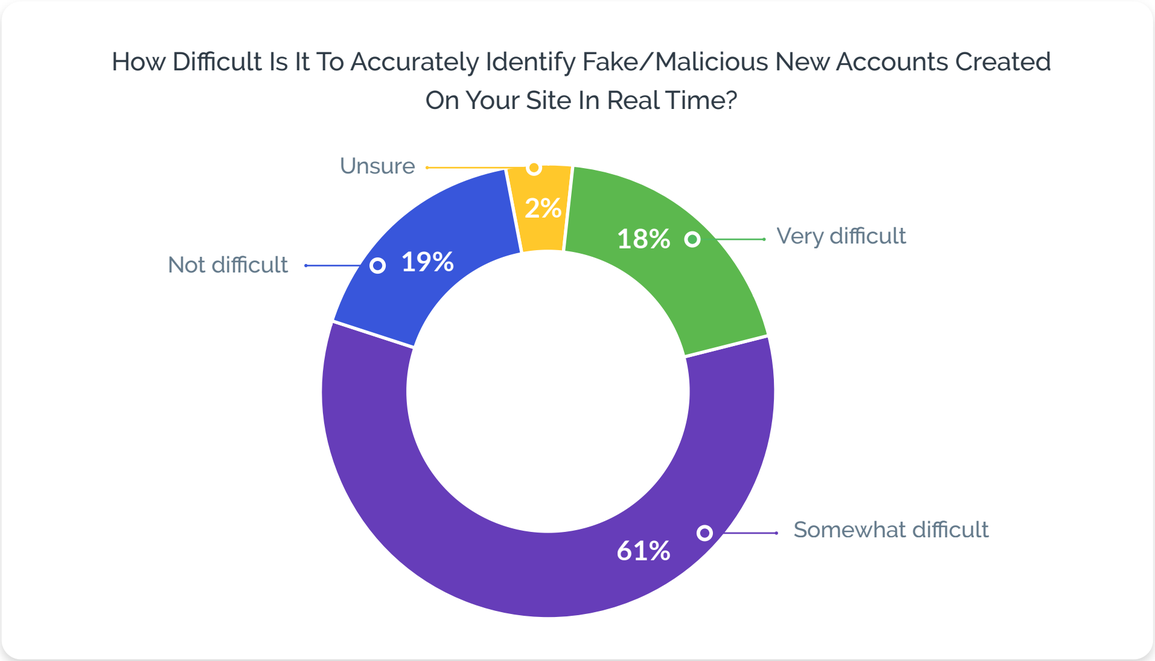
Founder and CEO

New account creation fraud powers a wide range of downstream fraud attacks, which is why it is so important to stop it before it happens and cause problems for businesses and users.

A Difficult Problem to Detect

One of the biggest difficulties in stopping fake new account creation is detecting it in real-time. Fraudsters deploy automation to create new accounts at scale in mere seconds, which are then used to commit numerous types of fraud before businesses even realize what has happened. And new account fraud is on the rise, with the Arkose Labs Network detecting four consecutive quarterly increases, culminating with more than 150 million such attacks in Q1 2021.

According to our poll, many companies face difficulties in detecting these attacks. . Nearly 80% of respondents said it was either “moderately difficult” or “ very difficult” to identify fake new accounts created on their site in real time. This is especially true for larger businesses, which have massive amounts of traffic coming to their site daily, and fraudsters use tools to “blend in” with the good users and avoid detection.



Intelligent Bots Make Detection Difficult

Advanced bots that appear as human traffic and seek to blend in with good users are becoming more prevalent as well as cheaper and easier for fraudsters to acquire and deploy.

Overwhelmingly, respondents to the poll cited these sophisticated bots as the most difficult to detect. This is a major concern because they can be deployed at such a massive scale, and evade detection while slipping through fraud defenses.

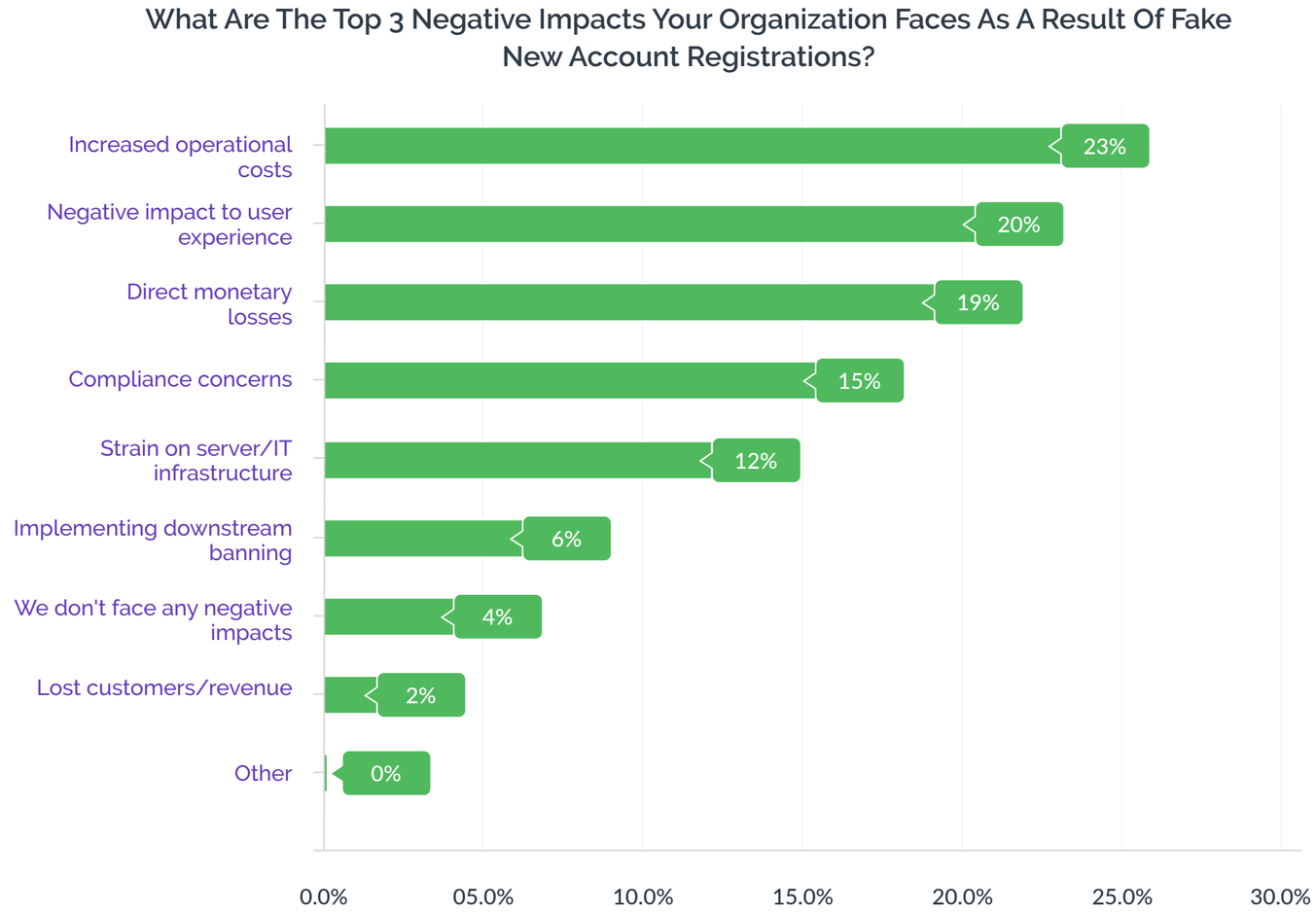
These types of bots can run JavaScript and can be programmed to simulate human behavior all the way to key presses, mouse movements and clicks, making them very difficult to detect.

New Account Fraud Has Wide-Ranging Costs

Fake new accounts, once created, create a multitude of headaches and costs to businesses. In our poll, increased operational costs was cited as the top negative impact of fake new accounts. These costs can include increased manual reviews, instituting “ban waves” to get rid of bad accounts as well as server costs to due increased traffic.

User experience is also greatly impacted by fake new account fraud, most notably when businesses have to add friction to the sign up process in order to stop bots from signing up for accounts. While this can be somewhat effective, it also dissuades many good users from creating accounts with businesses.

Increased compliance concerns and direct monetary losses -- such as when bot-powered fake accounts take advantage of promotional new sign up offers -- are also among the negative impacts of NAO fraud.

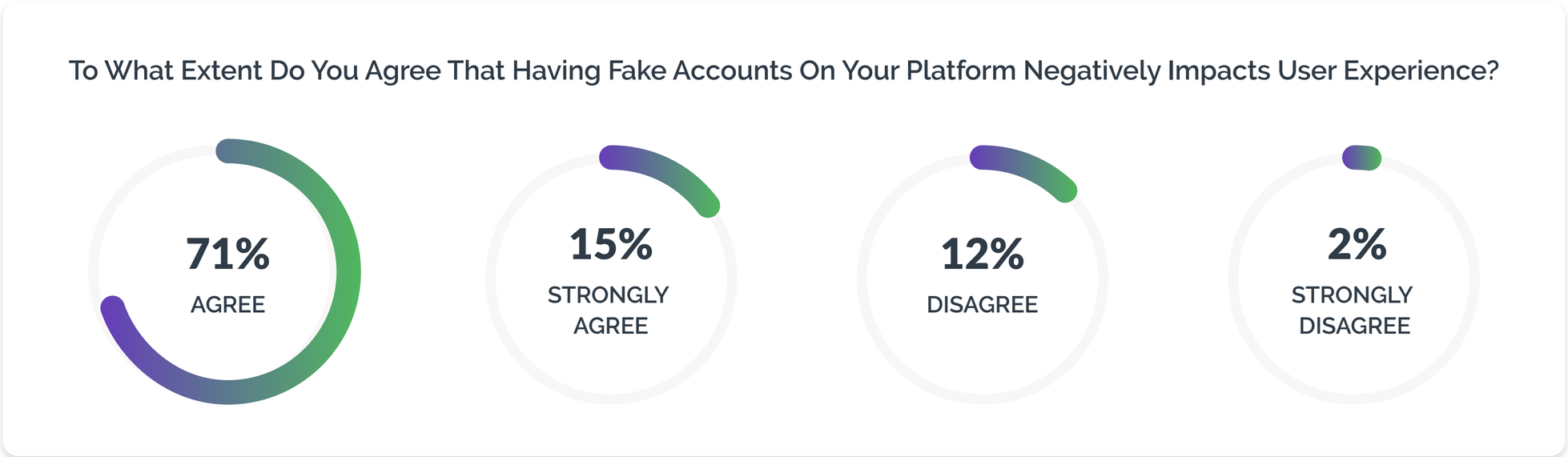


NAO Fraud: Severely Hindering the User Experience

Fake new account fraud not only carries a great businesses cost, but severely impacts the user experience as well. Nearly 90% of the respondents in our survey either “agreed” or “strongly agreed” that fake accounts on their platform impacted user experience.

As mentioned, this can include having to add more friction to the sign up process, but also involves fake accounts sending phishing and spam messages to good users. Social media and dating platforms, especially, are used by fraudsters to send messages to users from fake accounts, usually to extract money or get them to download a malicious link.

Furthermore, a little more than half of the poll respondents cited fake new account creation as a top user security concern. This only adds to the importance of stopping fraudsters from creating accounts.

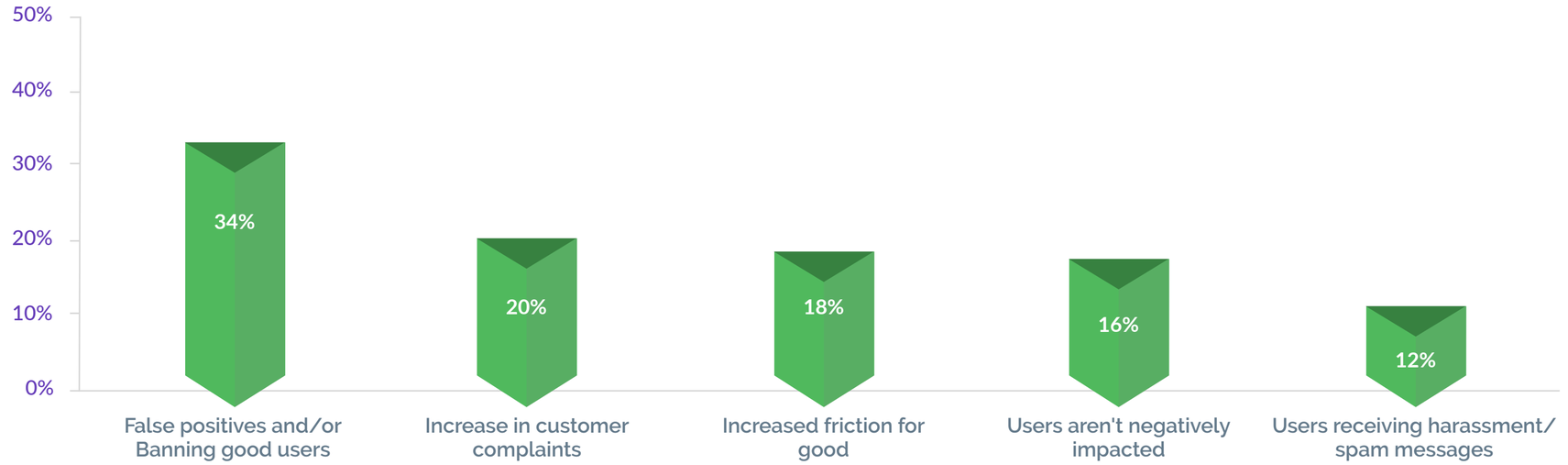


A Many-Layered Impact to User Experience

Too many false positives and accidentally banning good users were cited as the top negative user experience of NAO fraud by poll respondents. This not only affects the bottom line for businesses, as paying customers are unable to access the platform, but also can lead to negative brand reputation. Good users who are blocked or banned will voice their complaints on public forums, such as social media, message boards and online review sites.

An increase in customer complaints is another top impact of this type of fraud. Whether they are inadvertently blocked, or are the recipient of bot-powered spam and abuse, they will flood contact centers with calls. This creates operational costs for businesses, as overwhelmed customer service centers cannot respond to the increase in calls, as well as angry customers waiting on long hold times to speak to someone.

What Is The Biggest Impact Users Experience As A Result Of Fake/Fraudulent New Accounts Being Created At Your Organization?



Spotlight on: Online Gaming

The video games industry is one that sees among the highest amounts of new account origination fraud attacks. This is because there are numerous types of fraud that bad actors can engage in once they have successfully created fake new accounts. A common -- and persistent -- example is when fraudsters deploy bots to create new accounts, and then use these automation-powered accounts to farm in-game items, currency or level up characters. Obtaining such assets normally requires effort: they are the reward for players spending hours of in-game grinding, completing missions or other tasks. However, since attackers deploy bots at scale to perform the same repetitive actions over and over again in order to quickly accumulate in-game currency or valuable items or weapons, they can accumulate these assets in a manner that is against the spirit of fair play. Since bot attacks are generally inexpensive and easy to deploy, the fraudsters can then turn around and sell these valuable assets for much cheaper than they would normally go for on third party sites, and still earn a profit.

Fraudsters also use fake new accounts in order to utilize hacks or cheats to manipulate the gaming environment to their advantage. When they are reported by other players and found out, and their account gets banned, they can easily, and continually, create new accounts to engage in the same behavior. Bad actors also use fake new accounts to send spam or malicious messages to other users on the gaming platform, such as phishing messages trying to obtain personal information, or getting them to download a malicious link of some kind.

Spotlight on: Media and Streaming

Media and streaming services faced the highest amount of NAO fraud of any industry as recorded on the Arkose Labs Network, with more than 50% (53%) in 1H of attacks being of this variety. Streaming services see a high amount of fake new accounts as fraudsters seek to take advantage of promotional offers meant to attract new customers. Fraudsters can accrue free weeks or months of access to streaming services, and either use it for themselves or resell it to others. This deprives streaming companies of revenue and potential new customers.

Social media companies also face significant threats from NAO fraud. Bad actors create new accounts for a variety of reasons; these can include to spread disinformation or influence real users, to artificially like or prop up existing accounts, or to send spam and phishing messages. Such activity threatens to severely diminish the reputational integrity of the platform and hurt good users.

In many of these cases, the return on investment isn't as high for the fraudster as it is in attacking other industries. But since they can create fake new accounts cheaply and at scale, fraudsters can still make a good profit.

Case Study | Outlook.com

Microsoft Outlook needed a new way to stop fraudulent new account creations while improving customer experience - all in a cost effective manner. This was important not only to protect their own users but to create a safer environment for the wider ecosystem. Microsoft deployed the Arkose Labs platform to differentiate between good users, bots and malicious humans in order to eliminate spam and abuse. New users were shown enforcement challenges when sending their first email. The team implemented custom rules and policies to detect anomalous and suspicious behaviour, with challenges being presented whenever there was evidence of downstream large-scale abuse or spam.

The result was a 33% improvement in good customer throughput. There was a 93% reduction in fraud and abuse, with malicious users being prevented from carrying out large-scale attacks after setting up new accounts.

Business Problem

- Large-scale fake account registrations.
- Email accounts used for malicious and fraudulent purposes
- Fraud mitigation disrupted good user experience

Solution

- Unified authentication for new users
- Innovative challenges to stop bots and fraudsters
- Malicious emails detected and challenged downstream

Results

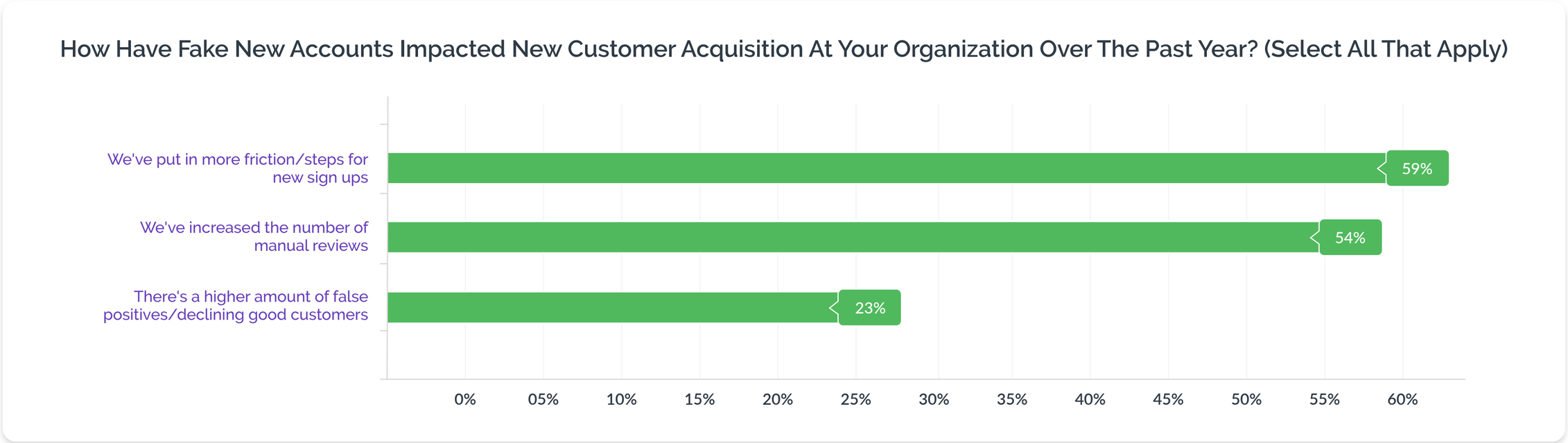
- 33% improvement in good customer throughput
- 98% reduction in fraud and abuse
- Stopped customer complaints about SMS verification

A Hindrance to New Customer Acquisition

To compete in today's digital economy, businesses need to enable a seamless, easy digital sign up process. Consumers do not want to be inconvenienced in any way.

However, fake new account fraud severely impacts digital new customer acquisition. Poll respondents listed several negative impacts in this regard, including having to implement more friction or steps in the new account sign up process, increasing the number of manual reviews -- which slows down the new sign up process -- and having to decline good customers.

For businesses, such measures can be devastating. In today's instant, always-on digital world, consumers will often abandon a sign up process if it creates too many steps or takes too long. What could become loyal, longtime customers are then lost at the very beginning of the relationship.



Fake New Account Attacks Continue to Rise

Over the past year, businesses across the globe have had to convert to digital models due to in-person restrictions and overall closures. Due to this shift, fraudsters have also learned to adapt and change their criminal tactics in order to maintain a worthwhile ROI.

As a result, many businesses have seen an increase in fake accounts: nearly 60% of our poll respondents reported some type of increase in this fraud.

It's also telling that none of these businesses that were polled are experiencing a significant decrease in fake account attacks. This means the problem is not going away anytime soon, and is only increasing. Businesses need to be vigilant about staying on top of fake new account creation before it becomes a big problem and disrupts their platform.

Has The Volume Of Fake New Accounts Created At Your Organization Increased In The Past 12 Months?

Conclusion: Creating a Safer Internet

It's difficult for businesses to identify and stop new account fraud because the fake account can often be masked to look like a real account creation. Of course, dumb bots are easily spotted, but today many attacks utilize more sophisticated bots that appear to mimic a good user. And human fraudsters performing multiple NAO attacks can hide or obfuscate their IP address, location or any other number of identifiers. The more sophisticated the form of fraud, the more difficult it is to detect.

That's why businesses need to take an evidence-based approach, where targeted authentication can be deployed to suspicious traffic in order to stymie automated attacks as well as slow down and frustrate human attackers. In this way fraudsters will be foiled, while good users will be able to easily sign up for new accounts and take advantage of promotional deals and other incentives designed to attract new customers.

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

About Arkose Labs

Arkose Labs

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.

Offices

San Francisco
250 Montgomery St 10th Floor, San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo