Arkose Labs

2021 STATE OF FRAUD REPORT

H1 Insights from the Arkose Global Network

Introduction: The Importance of Account Integrity

As we move further into 2021, it's clear that fraudsters have largely honed in one particular area of attack: digital accounts.

This is not surprising, as the transformation taking place in business has put the digital account squarely at the center of most consumers' lives. They are used to conduct business and commerce, store financial details, connect with friends and family, enjoy their favorite game or show, and so much more.

This year has revealed the critical need for enterprises to take a wider lens on fraud prevention - one that puts a high priority on securing accounts from being targeted by fraudsters. To date, about one-third of the attacks detected across the Arkose Labs network were fake new account registrations. Account takeovers, on the other hand, were powered largely by credential stuffing, with 285 million of such attacks detected in the first 6 months of the year.

Whether it be taking over existing user accounts, or creating fake accounts for a variety of purposes, fraudsters expertly disguise themselves as legitimate users to abuse and monetize digital accounts. With customer-centricity driving success in this digital world, businesses must enable a seamless account login or registration process, while still being vigilant at monitoring these touchpoints as the starting points of fraud.

This State of Fraud Report highlights key fraud trends uncovered from billions of sessions across the Arkose Labs global network to help businesses protect the integrity of user accounts before they can be used for malicious purposes.

Kevin Gosschalk

Founder and CEO

With customer-centricity driving success in this digital world, businesses must enable a seamless account login or registration process, while still being vigilant at monitoring these touchpoints as the starting points of fraud.

The Top 6 Fraud Trends of 2021

Prevalence of Credential Stuffing

With stolen credentials and sophisticated tech at their fingertips, fraudsters are continually profiting from high-volume credential stuffing attacks. Credential stuffing accounted for 5% of all traffic (good and bad) across the Arkose Labs network.

Surge in New Account Fraud

Fake new account registration comprised over one-third of attacks detected in 2021, an increase of over 70% from the end of 2020. Fake accounts contribute to increasing occurrences of in-platform abuse such as spam, phishing and info scraping.

Attacks Target Multiple Touchpoints

A diversification of attacks across user touchpoints highlights that attacks patterns are not always independent. More than ever, fraudsters are using registrations and logins in tandem to maximize their ROI.

The Maturation of Mobile

50% of all digital traffic (good and bad) originated from a mobile device, up from 35% in the second half of 2020. With an average mobile attack rate of 24%, businesses must be increasingly aware of attacks originating from mobile devices.

Spike in Human-Driven Attacks

The first half of the year delivered a 77% increase in human-driven attacks to supplement bot attacks. This is part of a growing trend towards hybrid and human-assisted attacks at scale.

New Attacks Out of Asia

Asia overtook Europe as a top fraud hotspot - despite continued malicious activity originating from Russia. China and India are back on the map as top originators of fraud attacks, alongside Vietnam.

2021 Attack Trends at A Glance

H1 2021 Attacks

15%
Attack Rate

Up to **100M attacks** in a single week

Human Attacks vs Bots

19%
Humans

81%
Bots

77% increase in human attacks over H2 2020

Mobile vs Desktop

24%
Mobile

76%
Desktop

50%
of all digital traffic from mobile devices

Regional Trends

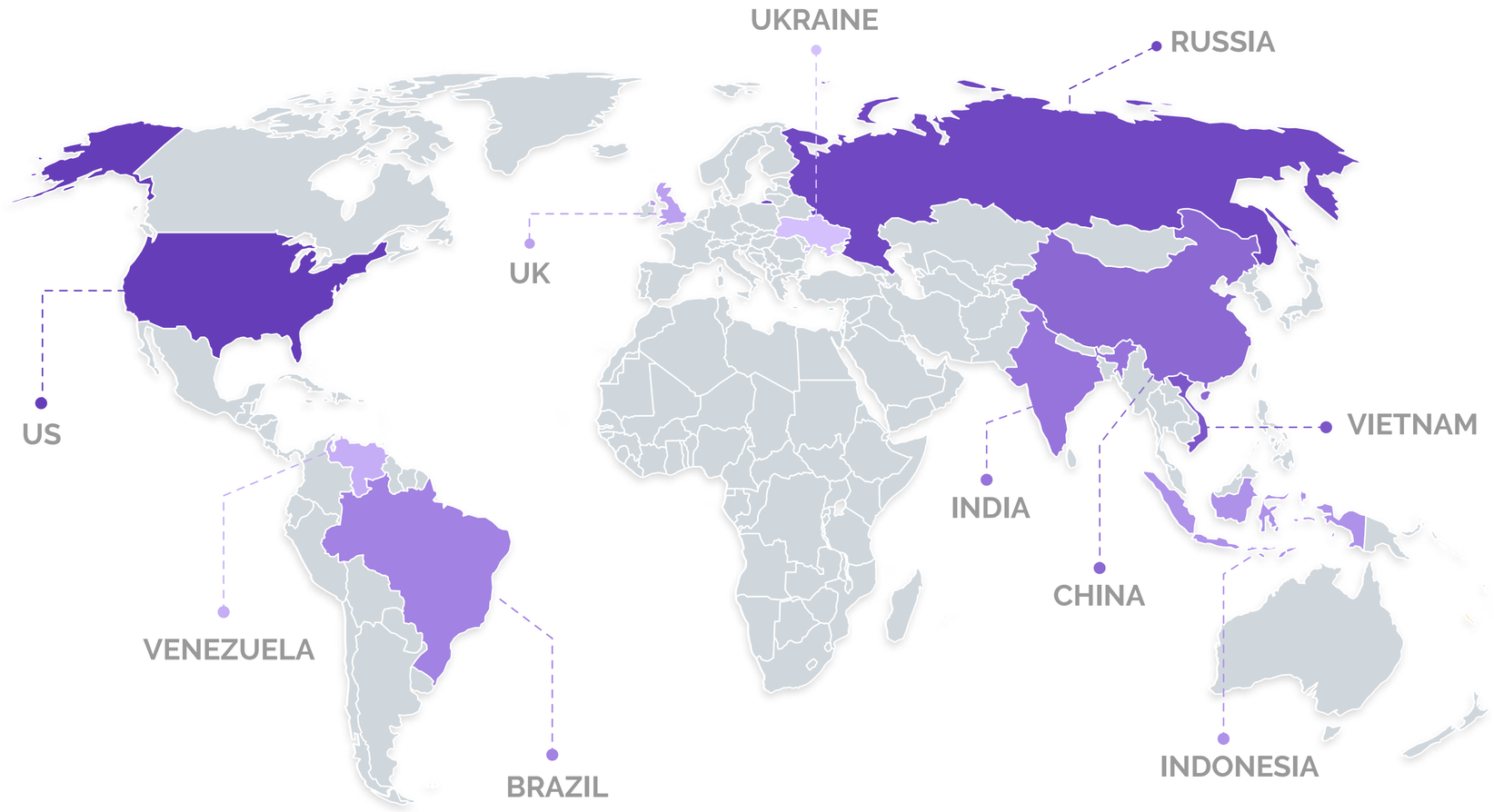
1/3
of attacks
originate from Asia

Vietnam and India
are top fraud farm countries

2021 Top Attacking Countries

Top attacking countries in 2021 are dispersed across North America, South America, Europe, and Asia, highlighting the truly global nature of the cybercrime ecosystem. The United States, Vietnam and Russia remained in the top 5 from 2020, while China and India surfaced as a key countries to watch. Newer players also emerged out of Venezuela and Ukraine.

Malicious actors in some countries concentrated their attacks on a particular industry. While China and Vietnam focused at least 50% of their efforts on the tech industry, actors from Russia and Brazil targeted gaming with ⅔ of their attacks.

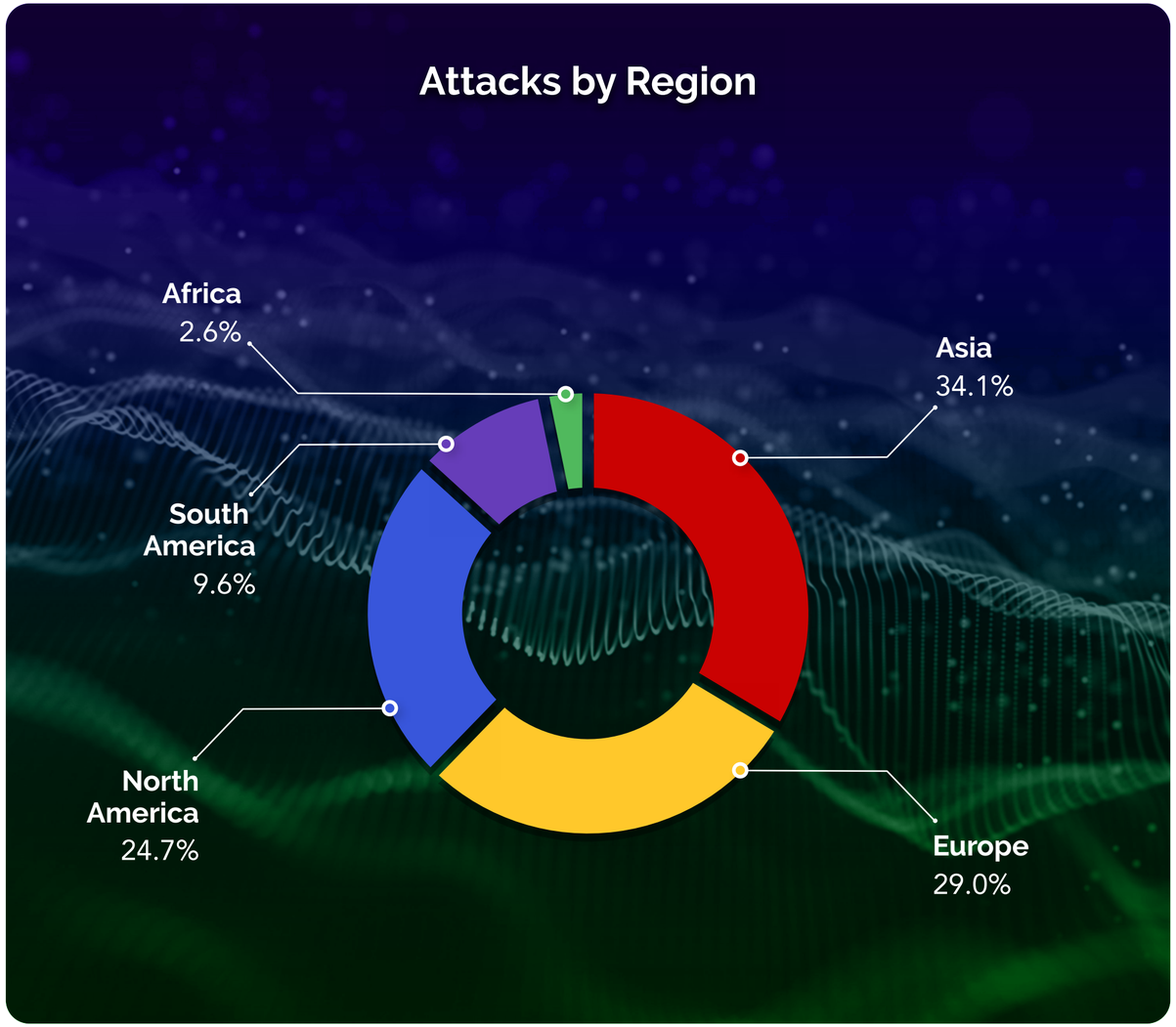


Regional Attack Trends

Asia was the top attacking region for the first half of 2021, followed closely behind by Europe and then North America.

Asia also had the highest percentage of human fraud farm attacks, with 60% of all such attacks originating from Vietnam and China. This illustrates this region's importance to fraudsters in finding human labor to deploy to supplement automated attacks, or to carry out tasks that require more nuance than bots can currently manage, such as sending phishing messages on online dating scams.

In Europe, attackers relied more heavily on automation to deploy efficient attacks that maximize ROI, such as credential stuffing.



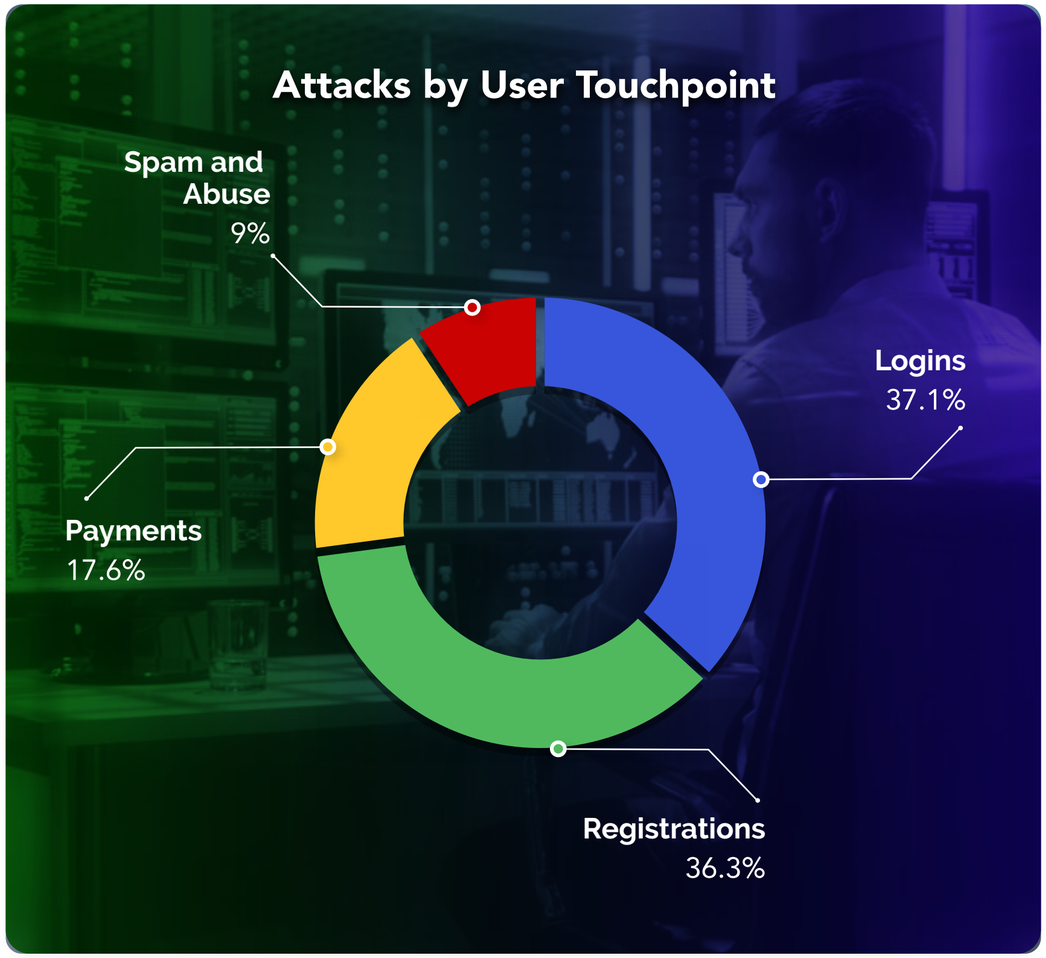
Attacks Target Accounts from Multiple Angles

Over the course of the first half of 2021, we've seen fraudsters deploy a mix of tactics aimed at account entry points. More than 1/3 of the attacks detected on the Arkose Labs Network were fake new account registrations.

Fraudsters are targeting existing accounts equally as strong with 37% of attacks affecting the user login point.

Trends across the Arkose Labs network show that attacks against logins and registrations are not always independent. In early 2021, the Arkose Lab team uncovered attacks on the registration flow followed immediately by an attacks targeting one client on the logins. A declined registration can validate if the account exists already, leading the bad actor to pivot to an account compromise attack.

As cybercriminals deploy these multi-pronged strategies, platforms must have an adaptable approach that protects both account entry points.



Credential Stuffing Attacks Make Up 5% of All Digital Traffic

In the first half of 2021, the Arkose Labs network detected and stopped 285 million credential stuffing attacks, with spikes upwards of 80 million in a single week. Considering it's large-scale, low-cost deployment, it's no surprise that credential stuffing made up 29% of all attacks. What's troubling is how these attacks have blended into increased traffic volume and account for 5% of all digital traffic. That means 1 in every 20 account logins could be an attack mimicking a real user.

Credential stuffing continues to be a prevalent attack tactic for businesses to keep an eye on. Their low barrier to entry makes them easy to deploy and fraudsters can generate profits with one successful compromised account. Their volumetric approach can come on abruptly, quickly overloading servers and putting users and the user experience at risk.

Fraudsters use credential stuffing attacks to take over real user accounts, which they then monetize in a number of ways. These include draining compromised accounts of funds, stealing and reselling personal; data, selling lists of known verified username and password combinations and using the compromised accounts to launder money gained from other illegal enterprises.

Credential Stuffing Over the First Half of 2021

29%
of all attacks are credential stuffing

285M
attacks

5%
of all traffic is a credential stuffing attack

The True Costs of Credential Stuffing

With credential stuffing on the rise, it's important to examine the full cost to businesses and consumers that these attacks bear. These include not only direct losses, such as lost revenue, but downstream costs such as impact to brand reputation, operational costs and more. Then there are legal and potentially regulatory ramifications as well for businesses that fail to safeguard user accounts.

Direct Losses

- Credential stuffing attacks cost the average business $6 **million per year** [1]
- The cost to companies to reset just one compromised password is $70 [2]
- 46% of businesses say that credential stuffing has led to decreased revenue [3]

Operational Costs

- Nearly half of businesses spend 1-5 **hours** remediating each incident of a compromised user account [4]
- It can cost upwards of $2 **million per year** in call center costs helping customers reset passwords [5]
- Businesses spend more than $1 **million** globally on botnet solutions to defend against credential stuffing [6]

Brand and UX Costs

- 60% of businesses said that credential stuffing attacks impacted brand experience [7]
- 33% of businesses face brand reputational damage from data breaches [8]
- 90% agreed that these attacks negatively impacted user experience [9]

Social Network Sees 1.5M Credential Stuffing Attempts in 1 Week

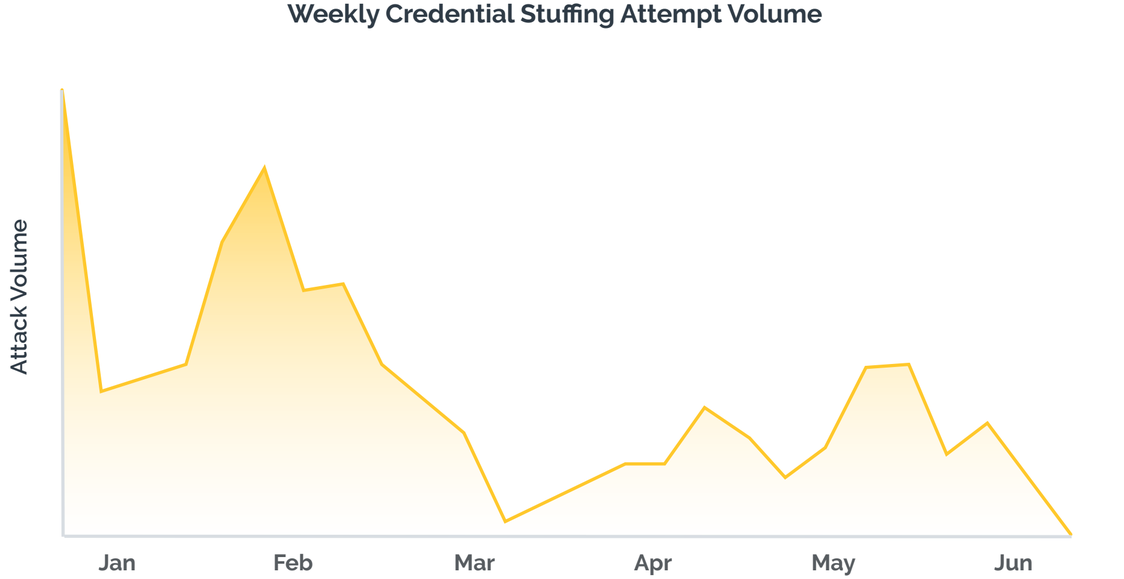
More than most industries, social media is powered solely on trust. Consumers trust that they can freely speak their mind and share details of their personal and professional lives on a secure forum. Any breach in account security can massively disrupt the integrity of the platform. One of the most prominent social media networks was a top target of credential stuffing attacks on the Arkose Labs network, experiencing upwards of 1.5M attempts in a single week.

Solution:

The social network chose Arkose Labs for its dynamic attack response. The major fluctuations in attack levels were addressed with increasing levels of pressure targeted at the tell-tale signs of credential stuffing traffic.

Results:

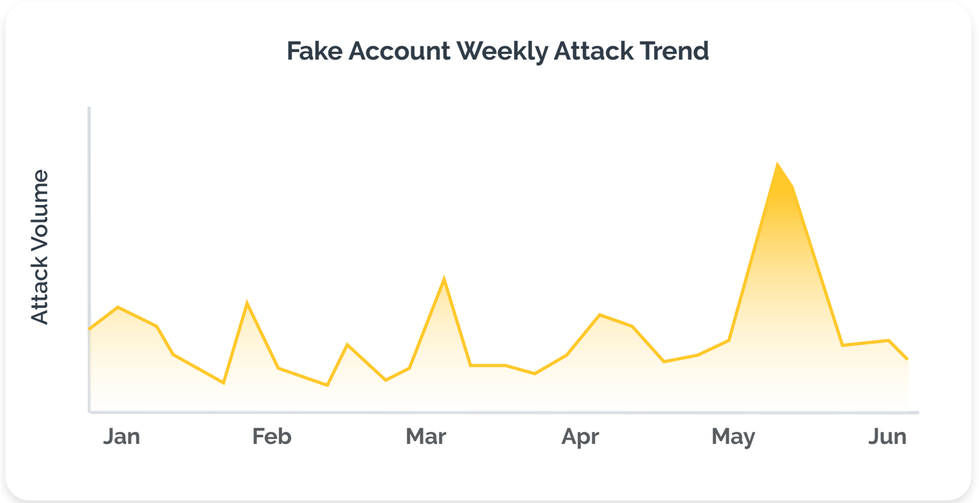
Attack volumes tapered off as attackers met resistance from Arkose Labs that undermined the ROI of their attacks. With support of the Arkose Labs team, the social network was able to efficiently protect their users from falling victim to account compromises.



New Account Fraud Increases by 70%

Logins have traditionally stood out as the most attacked customer touchpoint across the Arkose Labs network. However, the first half of 2021 has shown a rise in new account fraud to meet the levels of login-related attacks. Registration attacks increased 70% over the latter half of 2020, climbing up to 43M attacks in a single week at its peak.

With businesses working hard to increase customer loyalty in a competitive digital market, account creation is a key part of enhancing customer lifetime value and encouraging repeat business. Sign-up incentives that successfully attract consumers attract fraudsters equally. The registration process is abused by attackers using synthetic or stolen credentials to monetize bonuses and infiltrate platforms. This can lead to a wide array of downstream fraud like spam, phishing, and carding that's often harder or more expensive to block and can leave a blemish on a brand's reputation.



Businesses Struggle To Detect New Account Fraud

In an attempt to gain more insight into how businesses are grappling with fraud attacks today, Arkose Labs polled 100 IT executives on a range of topics. One notable trend was that many businesses are having trouble detecting and stopping fake account registrations on their platforms.

According to our poll, nearly 80% of respondents said it was difficult to some degree to identify new account fraud 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 to avoid detection. Once fake new accounts are created, fraudsters can commit a wide range of attacks with them, including spam, phishing, info scraping, inventory hoarding and more.

Intelligent Bots Power New Account Fraud

Detecting new account fraud can be difficult due to advancement in trained bots, which can most often appear as “normal” human traffic. Bots can be programmed to run JavaScript and simulate human behavior all the way to key presses, mouse movements and clicks

Overwhelmingly, respondents to an Arkose Labs poll on this attack vector 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. More than half of the companies polled responded to this attack pattern with more steps in the registration process or more manual reviews. Security and identity teams continue to make trade offs between operational efficiency and user experience in an effort to confidently stop fake account creation.

The impact of increasing new account fraud

59%
increased friction or steps for new sign ups

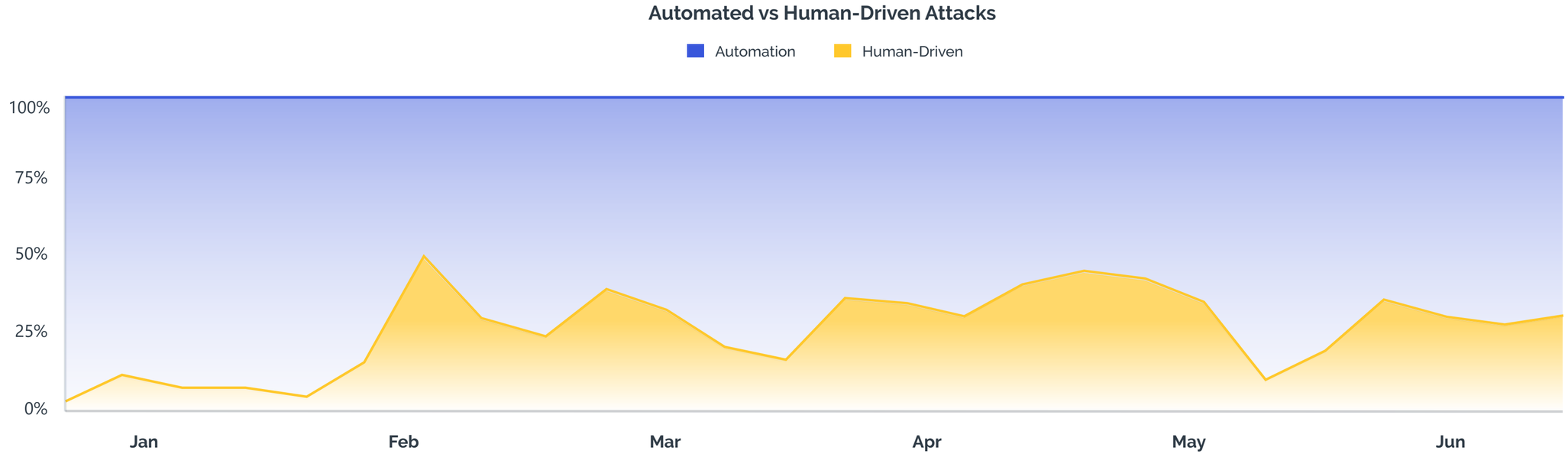
54%
increased the number of manual reviews

23%
saw higher false positives or conversion impact

Humans vs Bots: Major Increase in Human Attacks

The more efficiently fraudsters can execute attacks, the higher the potential ROI. The end of 2020 saw a surge of large-scale bot attacks capitalizing on the holiday season and digital transformation across industries at high volume. This never-before-seen uptick in human attacks is something to prepare for as we head into the latter half of the year. Human-powered attacks have been notoriously low in the past but now are becoming a legitimate concern as fraudsters circumvent increasing bot prevention with mal-intended humans.

While fraudsters still favor automation to deploy attacks cheaply, the volume of human-assisted attacks have increased dramatically over 77% since the second half of 2020. These types of attacks have been increasing the most in gaming and tech industries. Areas of the world that have seen the greatest rise in human attacks are countries in Europe, North America, and Asia.

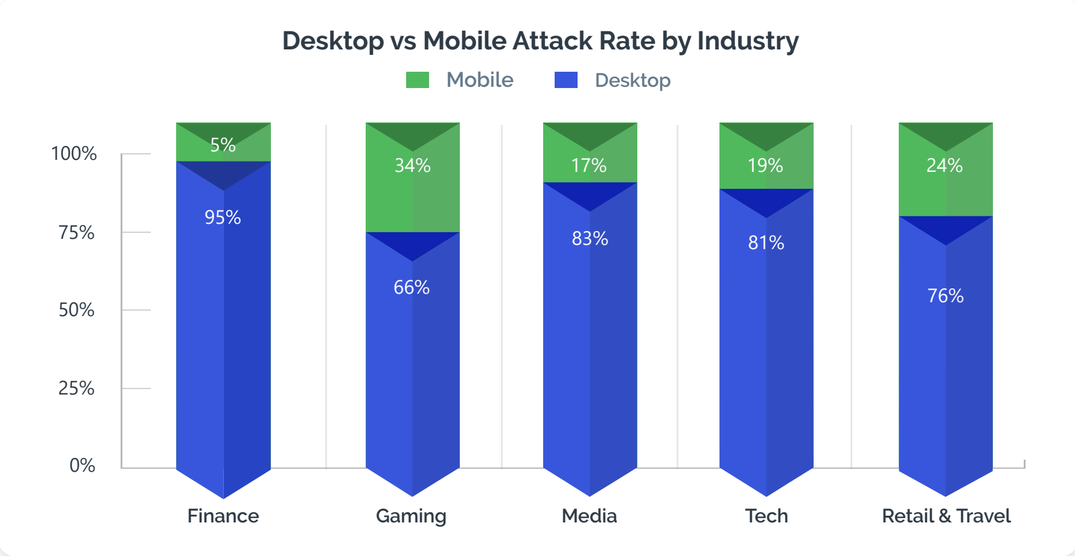


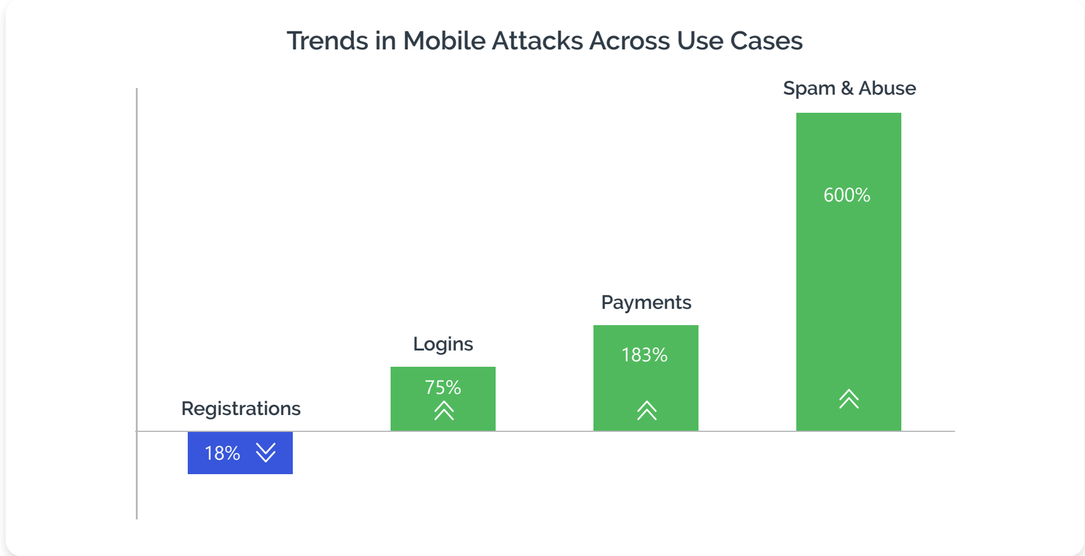
Attackers Quickly Adapt To A Mobile-First Marketplace

As mobile devices continue to be a more predominant channel for consumers to repeatedly access and interact with their favorite platforms, fraud is following suit to blend in with “normal” consumer behaviors.

2021 has seen the mobile attack rate increase to more than a quarter of attacks, up 40% from the end of 2020. Industries like gaming, retail, and travel are experiencing above average mobile attacks as people have settled into shopping and playing games out of the palm of their hands. Attackers are leveraging mobile usage across a multitude of touch points such as logins, in-platform abuse, and transactions which saw massive spikes in this attack type.

Mobile attacks can be deployed with device spoofing as numerous websites sell IP addresses with the appropriate device fingerprint. Unearthing malicious intent requires a storytelling approach that connects data signals. If the user's device says it's in Los Angeles based on the locale and time zone, but the IP address is coming from Europe, the story doesn't check out.





Financial Services Targeted for Application Fraud and ATOs

1 in 7
attacks target logins

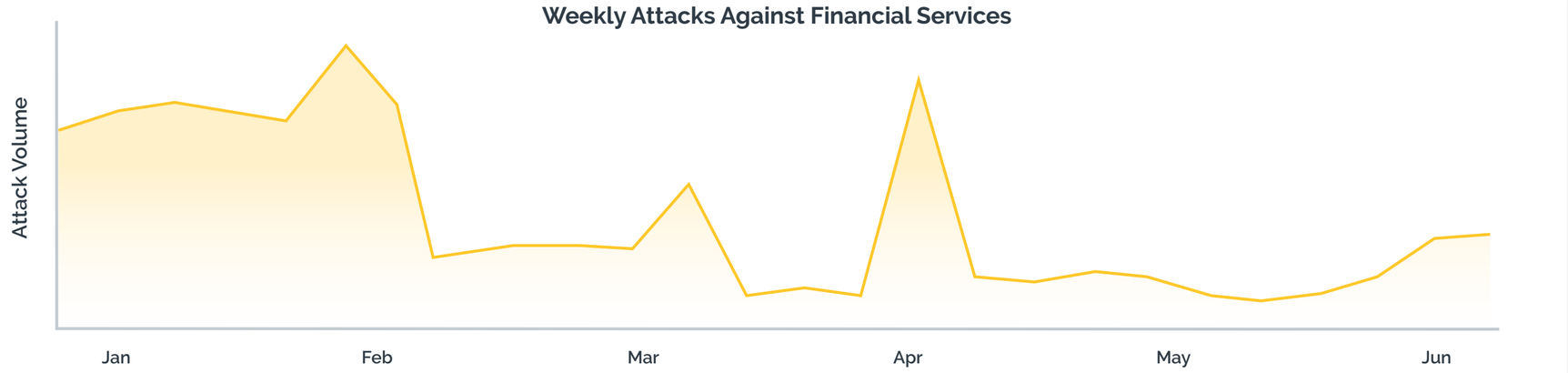
Application fraud
most attacked customer touchpoint

95%
desktop vs. mobile attacks

While financial services platforms were hit with fake credit cards, personal loan applications, and government subsidies in 2020, this year has brought a diversification of account-related attacks as digital identities have been continuously disrupted.

This year logins have emerged as an attack touchpoint to watch, largely driven by automated attacks attempting to confirm legitimate accounts and access customer funds. Meanwhile, cybercriminals are making it harder to detect a fraudulent application, leveraging stolen credentials to mirror a real person capitalize on sign-up bonuses, and simplified application processes.

Mobile attacks are still lagging behind desktop. However, we anticipate this to change as mobile-first neobanks and fintechs continue to gain market share, as consumers opt for mobile banking en masse.

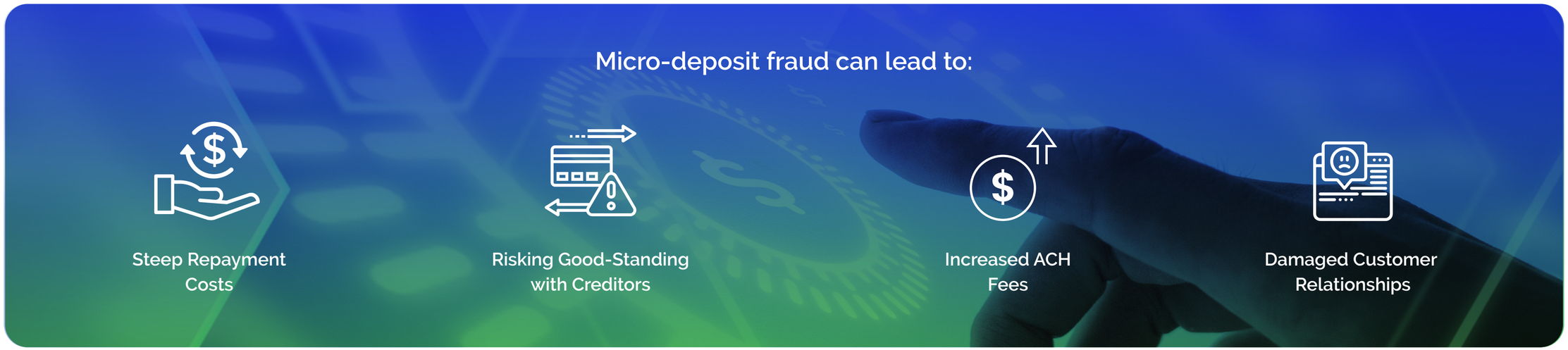


Spotlight: Micro-Deposit Fraud in Financial Services

As bad actors extend their attacks across an increasing array of customer touch points, financial services companies have mounting concerns around edge use cases - beyond traditional payments, application fraud and account logins. One example of this is the rise of micro-deposit fraud..

Companies in the financial services industry use micro-deposits as a security measure in the process of account verification. However, human fraudsters have been creating fake accounts to manipulate the micro-depositing process sometimes using stolen credit card information. If the credit card credentials are successful, the fraudsters will make mini deposits as low as $0.02 to a bank account they have already created. Although these deposits are less than $1, they can add up over time to create a multi-million dollar scheme.

With the rising use of fraud farms to mirror good user behavior, companies in financial services are left unprepared and vulnerable. Protecting high-value consumer accounts requires a new level of scrutiny to unearth human-driven fraud.



Gaming Sees a Rise in Mobile-Based Fraud

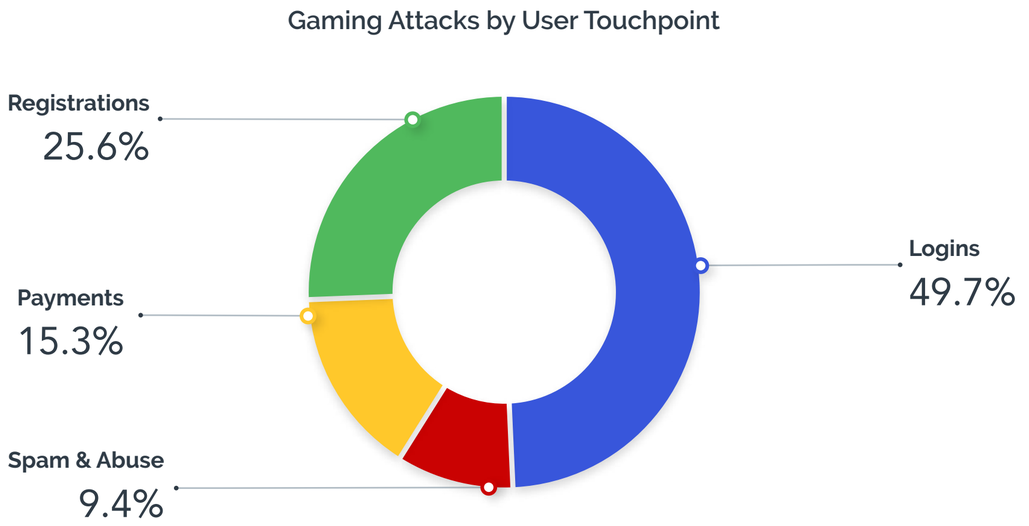
35%
attack rate

225M
credential stuffing attacks in 6 months

2x
mobile attacks over H2 2020

In the first half of 2021, the gaming industry saw 75% of attacks targeting the login and registration points. Registration is often carried out by human fraudsters which correlates with the huge spike in human-driven fraud. However, credential stuffing gaming platforms continue to be plagued by mass credential stuffing attacks, fielding nearly 225M attempts to access valuable player accounts since the beginning of 2021.

With the growing popularity of mobile gameplay, attacks originating from mobile devices grew 2x the amount seen during the second half of 2020. During the pandemic, the number of people playing video games, time spent in game, and in-game purchases increased exponentially. As a result, we've seen a larger share of attacks within games targeting in-game economies and valuable gamer assets than ever before.



High Rate of Human Attacks Target Social Media and Streaming

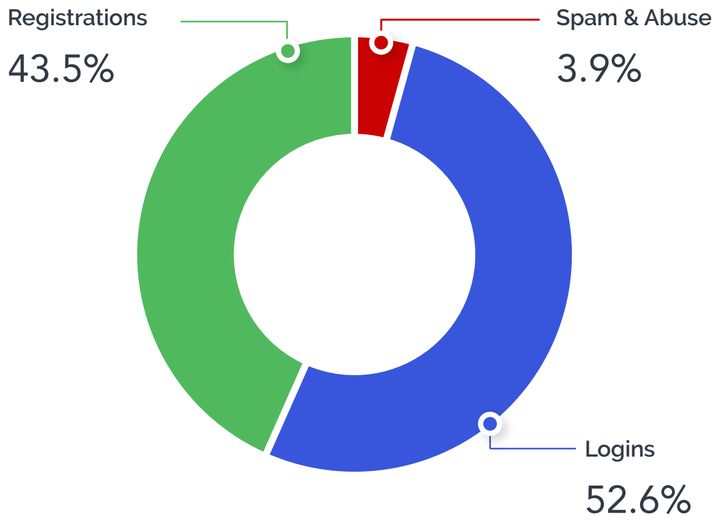
18%
attack rate

32%
of attacks were human-driven

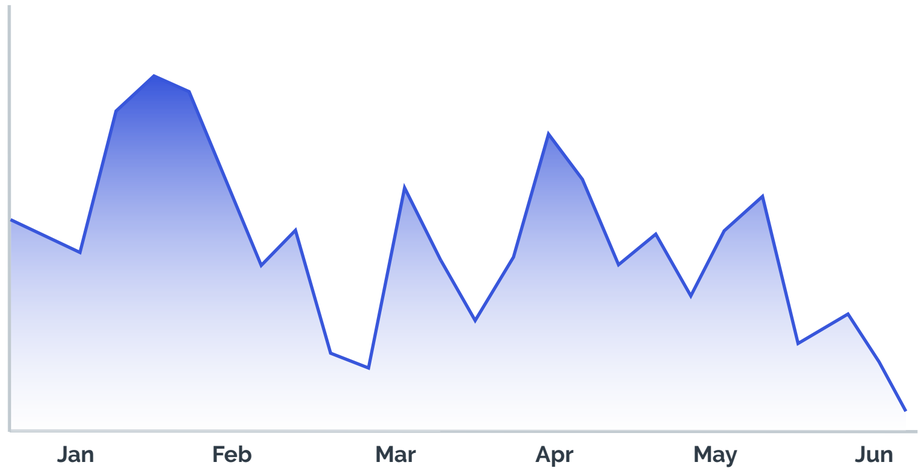
21%
mobile attacks versus desktop

Social media and streaming services have niche monetization potential for fraudsters compared to some other industries, but that doesn't mean they are ignored. Logins were the most targeted use case; fraudsters often seek to compromise the accounts of real users of a streaming service and resell access to numerous other people to make a profit. In social media, real accounts are often targeted to then disseminate spam phishing messages, and appear as if they come from a "real" person.

Attacks by User Touchpoint

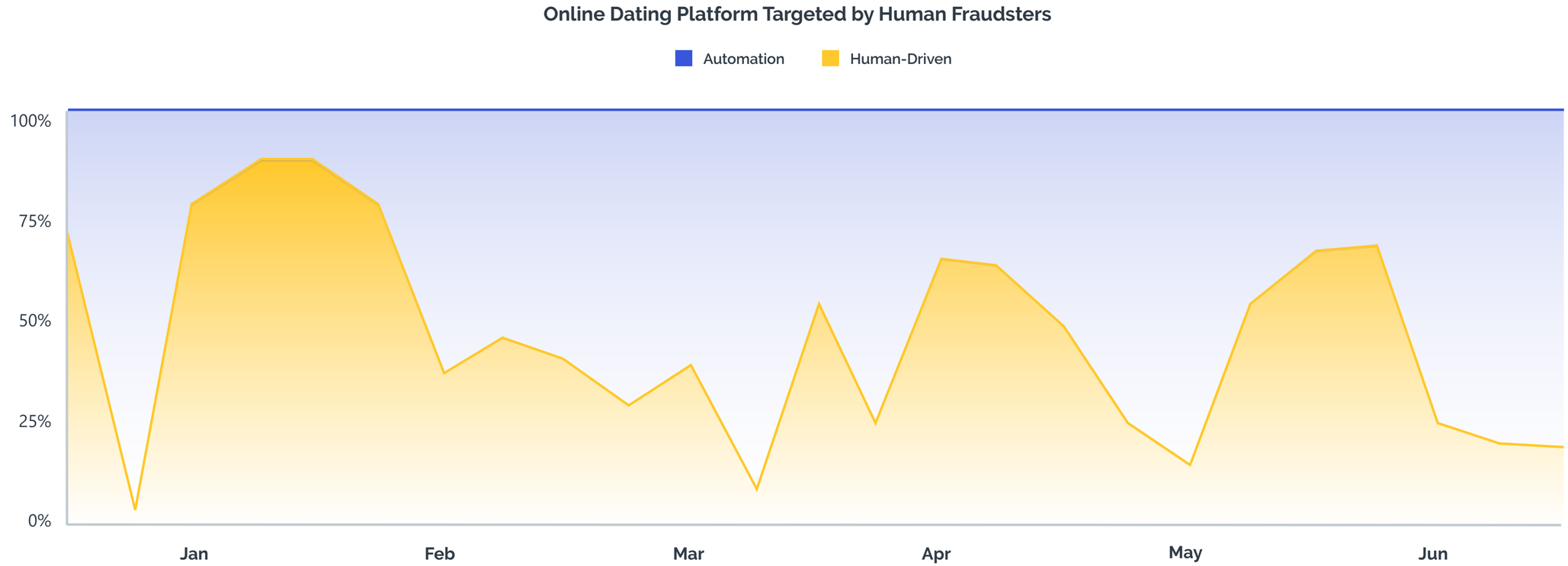


Weekly Attacks in Media & Streaming



Spotlight: Human Fraudsters Use ATOs for Romance Scams

The online dating industry saw some of the highest rates of human-driven attacks seen across many different industries. Up to 85% of all attacks seen in the dating industry were coming from human fraudsters. Human-driven attacks have been a minority of fraud cases for many past quarters and is usually far outnumbered by automated attacks. Seeing these unusual spikes is something the dating industry needs to prepare for. Human fraudsters use ATO forms of attack to carry out targeted romance scams and sell verified accounts for further abuse.



Tech Platforms Attract Freemium Abusers

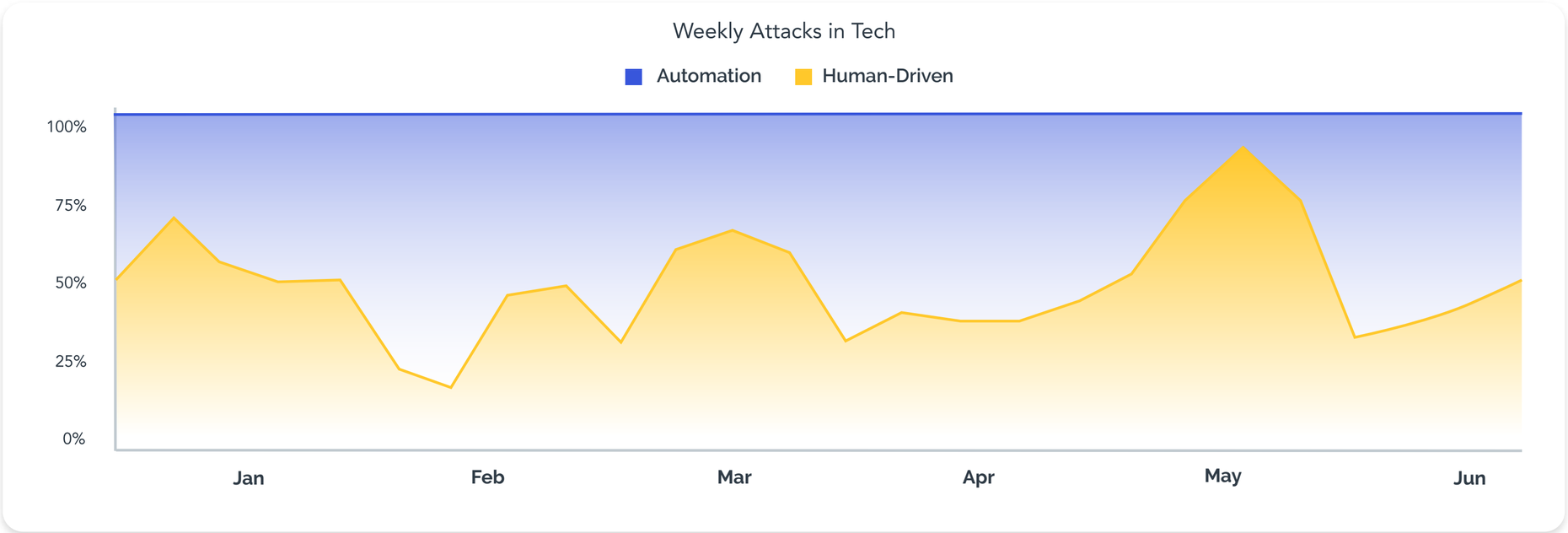
16%
attack rate

31%
human attack rate

1/2
of attacks from China and Vietnam

Attacks against tech platforms are almost exclusively focused on the login and new account registration point. Fraudsters frequently create fake new accounts on these platforms to take advantage of freemium and promotional offers for free server time, meant to attract new customers. They can then abuse these offers to conduct tasks that require a lot of computing power, such as mining cryptocurrency. This, in turn, strains the servers of tech platforms and affects good users.

Tech platforms also saw a relatively high average human attack rate at 31%. Even as tech companies invest in more innovative defenses, fraudsters from China and Vietnam are using the availability of fraud-farm workers to deploy nuanced attacks that circumvent detection measures.



Case Study: Cloud Data Platform Stops Crypto Abuse

Business Problem

The client, a premier enterprise software company that provides a cloud computing platform which allows teams of developers to engage in projects related to data engineering, data science, machine learning and more, was the target of fraudsters who would use both bots as well as human fraud farms to sign up for fake new accounts in order to abuse promotional offers for free trials meant to entice new customers. Fraudsters would use accounts with this free trial time in order to engage in tasks that required a high level of compute power, most notably mining cryptocurrency.

Solution

The company engaged Arkose Labs to be used as a first line of defense on the new account sign up flow. Arkose Labs was able to immediately stop nearly all of the malicious bot traffic and then helped the client stymie persistent human fraud traffic. Arkose Labs continually served up this traffic increasingly difficult or timed challenges designed to frustrate human fraudsters and make them give up.

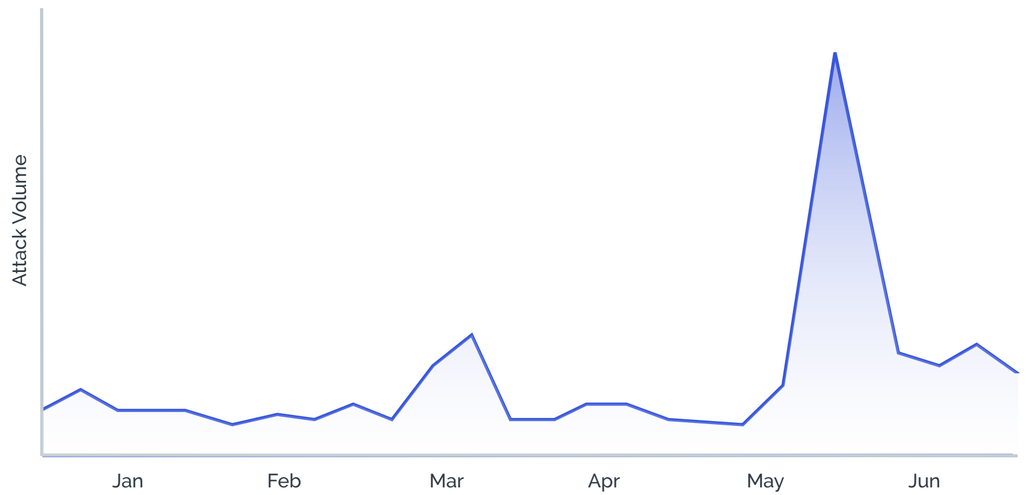
Results

Overall, these types of attacks were reduced by more than 95% since Arkose Labs was implemented. Furthermore, the measures that were used did not provide any hindrance to new customers signing up and taking advantage of promotional offers.

Case Study: Major Peaks in Attack Traffic on Tech Platform

Even though fraud prevention is a 24/7 job, fraud and security teams need to be prepared for extreme variations in attack volumes from week to week.

One major tech platform experienced 42.7 million attacks in a single week - 20x the attack volume over a couple weeks prior. The attackers hit the platform from multiple angles at once, with 80% of attacks aimed at the registration point and 20% at the login point. Whereas normally this company experienced a 70-30 mix of bot vs. human-driven fraud, this peak attack week was driven almost entirely by automated attack tactics. This can unexpectedly throw a team into a reactive, all-hands-on-deck mode to minimize any damages to their customers and experience.



Actionable Insights

- Ensuring equally-strong defenses staged at the most targeted attack points
- Having the added support from vendors to extend the team's manpower
- Employing scalable and adaptable attack response to increase pressure on attackers at any given notice

Scraping Attacks Emerge on Retail & Travel Sites

40%
attack rate

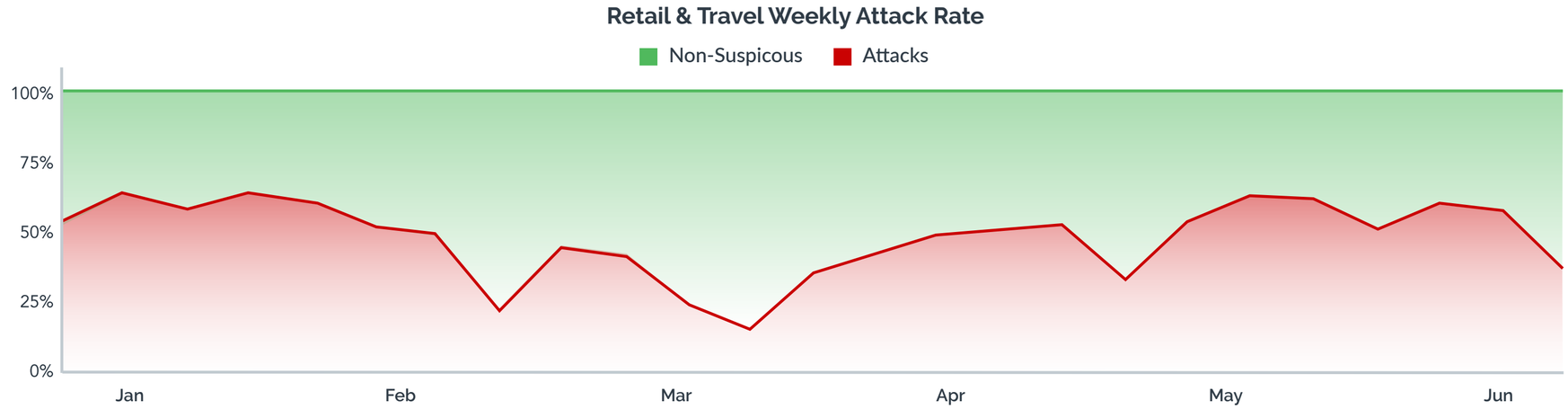
33%
of attacks were human-driven

27%
of attacks were scraping

The two industries that have not seen much of a break this year are retail and travel. 2021 has brought a consistent stream of attacks with an overall attack rate of 40%.

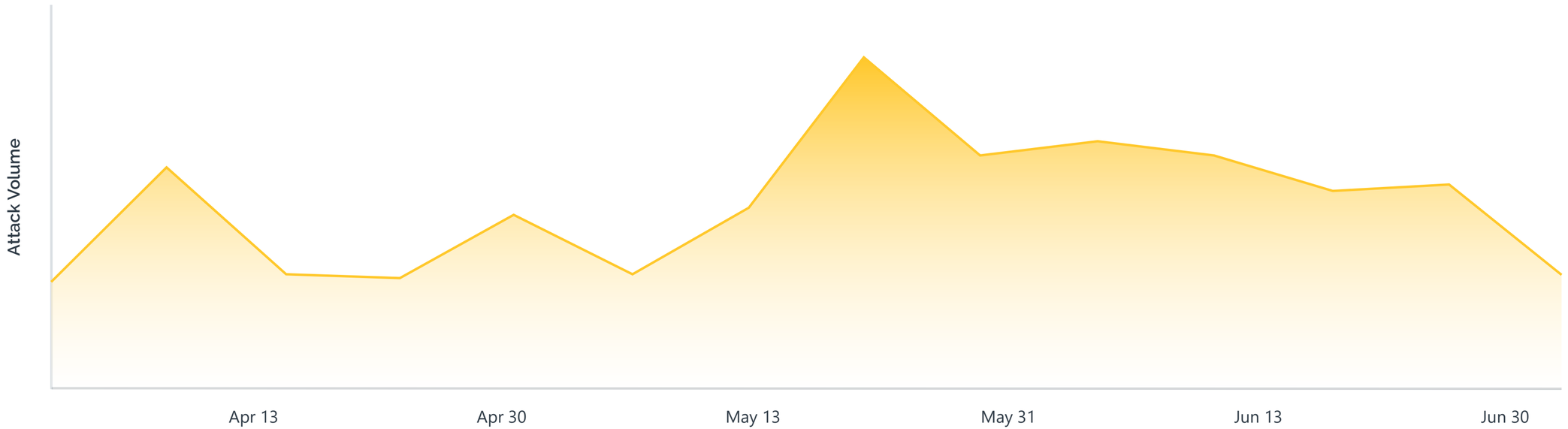
eCommerce sites have traditionally been a prime target for payment fraud, using stolen credit card credentials. However, retailers are also dealing with other bot-related attacks such as scraping and inventory hoarding, loyalty point theft, and gift card fraud.

With the world reopening and flights becoming more common, travel sites are being targeted again, after a reprieve at the height of the pandemic. Hotel and flight booking sites are being targeted with bot attacks, focused on unauthorized price scraping and inventory hoarding. These large-scale attacks risk overwhelming the sites and prevent genuine consumers from completing their purchases.



Case Study: Malicious Bots Up to 95% of Travel Site Traffic

Companies in the travel industry strive for a balanced look-to-book ratio which demonstrates how many people of those who visit the website actually make a purchase. If the ratio is off-kilter, it may cause a breach of contract between airline and hospitality companies. 95% of attacks on travel were automated scraping attacks looking to steal information, due to the sheer volume of these attacks at peak periods. These attacks remained high and persistent throughout Q2 and tailed off at the end of the quarter due to our consistent application of pressure against this malicious traffic. However, these scraping attacks have consistently made up 50% of all traffic seen on travel websites and sometimes reach up to 95%. Automated attack prevention is essential for travel companies in order to maintain a stable look-to-book ratio.



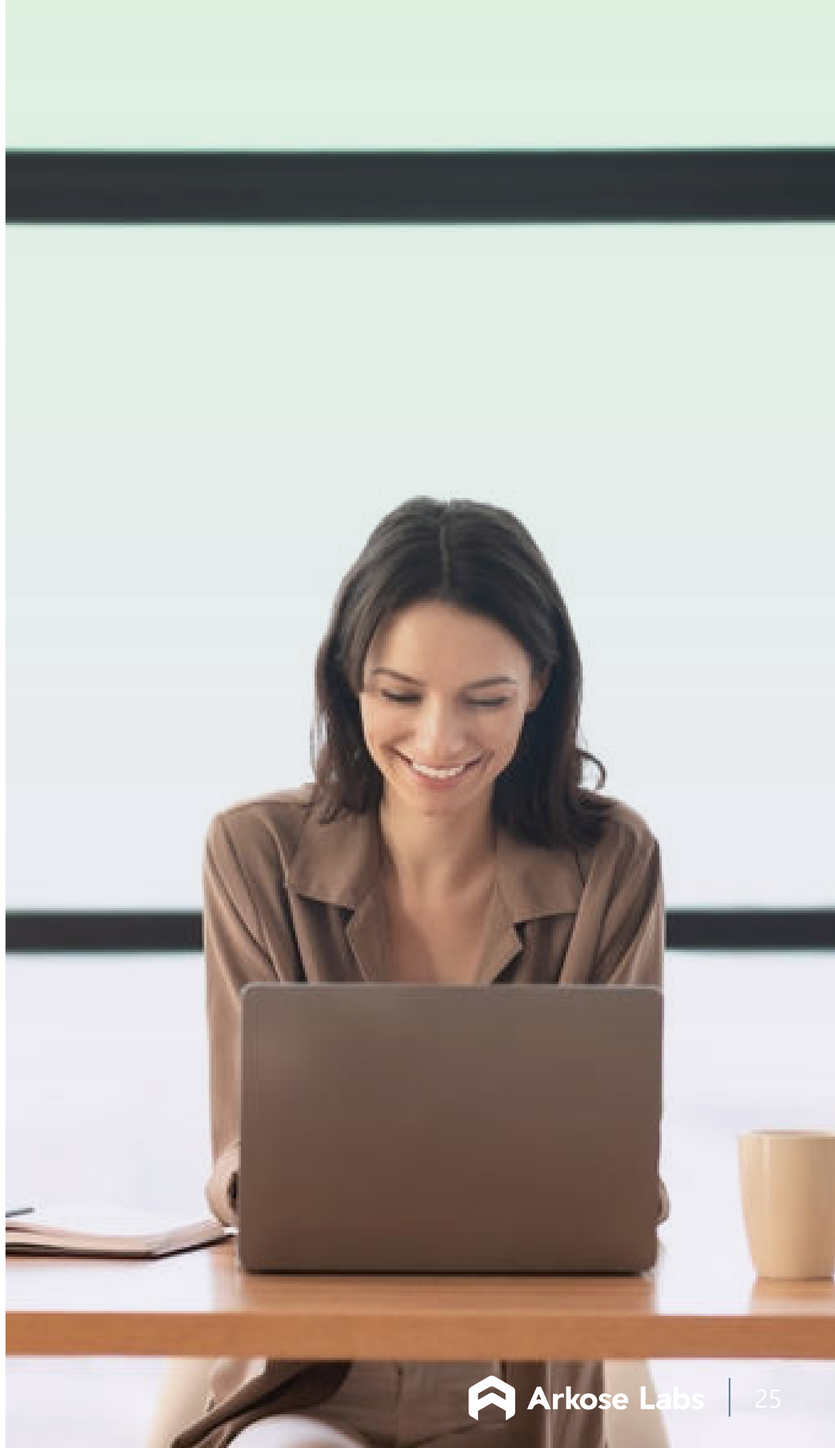
Conclusion: The User Account at the Center of Commerce

In many ways, the customer is at the center of the digital economy today. They expect a seamless personalized, customized experience from the businesses that they interact with. If they don't receive that, they have myriad other options they can do business with.

That means customer-centricity has never been more important to businesses. And to ensure a great customer experience, the integrity of digital accounts must be sacrosanct. A digital account is an integral part of a consumer's life; it holds financial information, personal data, and other private information. Businesses that fail to protect these accounts risk potentially losing customers.

Customers also want to be sure that any other person they interact with on a digital platform is who they say they are. Fake new accounts that go on to disseminate spam, send phishing messages to real users, or hoard promotional offers meant for real customers are a threat to any digital businesses, and failing to reign them in could mean angry customers and lost business.

The importance of account integrity will only increase over time, as even more of our everyday lives is conducted online. And attacks that target digital accounts will only continue to increase in both sheer numbers and severity. The companies that do the best job of maintaining digital account security will be leaders in the digital economy going forward.



Arkose Labs

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.

Offices

San Francisco
250 Montgomery St 10th Floor, San

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo