Arkose Labs

# Breaking (Bad) Bots: Bot Abuse Analysis and Other Fraud Benchmarks

Unique Insights from the Cybercrime Economy by Industry, Attack Type, and Region

Q4 2023

# Executive Summary

Cybercrime has become an economy unto itself, fueled by financially motivated bad actors building "dark" businesses and making lots of money. Cybersecurity Ventures estimates the cybercrime economy will reach $10.5 trillion by 2025. To earn as much as possible, bad actors are motivated to operate efficiently because the effort-to-attack ratio drives their "wages" and impacts their personal wealth creation.

Bots enable bad actors to attack efficiently and effectively. Within the last year, mainstream news outlets have covered bots being used to buy Taylor Swift tickets, the latest Nike shoe, or the new, rare Lego kit—only to be sold again for exorbitant prices. Around the holiday season these types of bots are jokingly referred to as "grinch bots," trivializing their material impact on legitimate consumers and businesses.

**In reality, the downstream effects of bot attacks aided by human fraud farms abet very dark activities,** which you can read more about starting on page 7. We observed a 121% increase in total attacks (bots & fraud farms) in Q2 over Q1 2023.

The bot problem is a weighty one that escalated exponentially in the first half of 2023—167% in Q2 2023. And when fraudsters' bots are blocked, they often pivot the attack to human fraud farms. This new analysis shows that human-based attacks increased 26% in Q3 over the second quarter time period.

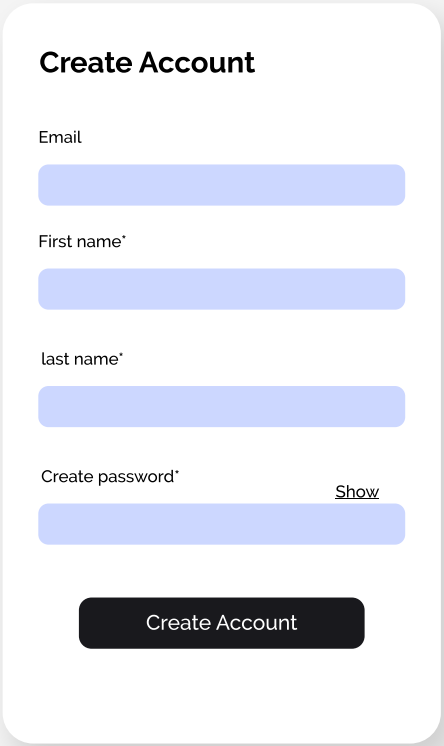
In this new analysis of bot abuse and human fraud farm actions, we reveal the top attacks by industry, type, and region. We also share insights on how these attacks happen and what can be done to detect and block them. Here's a hint: When the effort-to-attack ratio is too high, meaning it takes cybercriminals too much time and too many resources to break into an online bank account or deploy SMS attacks or scrape websites or test credit cards, they stop. They move on to less-protected businesses.

The data used to drive these insights comes from the Arkose Labs Global Intelligence Network, a consortium of the biggest companies in the world as well as category leaders that are Arkose Labs customers. These companies represent the highest-value targets that cybercriminals set their sights on. Our unique position to observe this activity informs the analysis throughout this study. It covers Q1, Q2 and Q3 of 2023.

# Dark Effects of Bot Attacks: It's not just Tickets, Toys, and Shoes

Every day, bad actors are deploying very sophisticated schemes using intelligent bots that contribute to and perpetrate crimes other than tickets, shoes, and toys – far worse crimes, crimes against humanity.

Typically the crime starts on a company's website or mobile app where, in normal circumstances, a legitimate person registers (or signs up) for an online account or signs in to an online account they have already created.




Take the U.S. banking industry as an example. It's estimated that 208 million online bank accounts exist today. To create those digital bank accounts, the consumer had to first register online with the bank. From a bad actor's perspective, that represents 208 million vulnerability points that can only be reached through the effective use of bots.

In Q2 2023, there was a 202% increase in bots attempting to take over consumer financial accounts, and a 164% increase in bots attempting to establish fake new bank accounts. This trend continued going into Q3, which experienced a 30% increase over the second quarter in fake new bank accounts. Bad actors were attempting to drain account balances through ATO attacks, while online fake accounts were most likely the preferred methods to launder illicit proceeds gained from real-world crimes like human trafficking, drug dealing, or weapon sales.

**202%**
increase in bot ATO attacks in financial services

**164%**
increase in bot-driven fake new bank accounts

In the first half of 2023, 21% of traffic going to dating sites was bad bot traffic. Bad actors primarily credential stuffed their way into consumers' existing accounts as well as created fake new accounts. But that changed dramatically going into the back half of the year. Fake account creations became the primary attack type, outpacing ATOs and increasing more than 36,000% in Q3 over Q2. The "why" behind

the stats is interesting and disturbing. What did financially motivated bad actors hope to gain by attacking dating sites? How do these actions lead to making money?

Bad actors were likely attempting to initiate money-making romance scams or worse. The Polaris Analysis of 2021 Data from the National Human Trafficking Hotline shows that dating sites were the number one locations for sex and labor trafficking recruitment (23%). Human trafficking is a very lucrative crime, reaching $150 billion in profit. But how is the money moved? Online accounts at banks, credit unions, and digital banks are often used as a layer in the money laundering process.

A chokepoint exists. Downstream crimes like money laundering can be stopped, when bad actors are stopped from making money that they need to move, for example. That happens when the effort it takes for a bad actor to take over online accounts and create phony accounts upstream is no longer profitable for them. This behavior is the fundamental principle Arkose Labs works from—make the attack too expensive for the adversary to continue. Here's what one attacker recently told investigative reporter Brian Krebs: "'My partners (I'm a programmer) lost time and money while Arkose Labs introduced new precautions on Twitter.'"

> **"My partners (I'm programmer) lost time and money while Arkose Labs introduced new precautions on Twitter."**
>
> - Quotpw (a cybercriminal)

# 2 Trends Empowering Cybercriminals

The surge in bot and human fraud farm attacks is driven by two technology trends.

### Generative AI

It's understatement to say the rapid proliferation of generative AI (GenAI) is transforming the landscape of cybersecurity. In fact, GenAI has lowered the barrier to entry for attackers, which, in turn, has quickly made it an imperative rather than an option for CISOs and their teams to attend to.

Our threat researchers have noticed a significant uptick in the last year, and especially in the past six months, of GenAI being used for content generation by bad actors. The immediate use has been to create pristine phishing emails, meaning the emails are perfectly worded – without the telltale grammar mistakes that, prior to GenAI, were a major phishing telltale. As 2023 closes, we fully expect to see a major increase in romance scams, because bad actors are using GenAI to craft perfectly worded responses on dating apps and sites. We've observed them using bots to scrape content from websites to then tune GenAI models (read more in the sidebar about this troubling phenomenon).

GenAI has unleashed web scraping attacks. An attack once confined primarily to the travel, e-commerce, and gambling industries has now expanded to all verticals, as fraudsters use bots to scrape public and personal information from websites and then use that data to tune their GenAI models. Our threat researchers have observed three important landscape changes:

1. The evolution of simple scrapers to ATO class infrastructure.
2. An increasing number of commercial scraper services.
3. Developer groups scraping data for GenAI apps.

Analysis shows that scraping is now one of the top five most popular attacks for all industries and increased 432% in Q2 over Q1 2023, making scraping the fastest-growing attack type (see page 8). Scraping remained a top five most deployed attack by fraudsters in Q3 and has quickly become a new problem for the social media industry, increasing 11% in the second quarter. Also of note is that 100% of these scraping attacks were perpetrated by bots.

**100%**
of scraping attacks perpetrated by bots

### Before GenAI there was (and still is) DIY Fraud

Cybercriminals are rapidly advancing their skills by embracing DIY Fraud, which is also called cybercrime-as-a-service (CaaS), deploying bots and unleashing a wave of attacks on enterprises, causing trillions of dollars in damages. This shift lowers the barrier to entry and grants access to cybercrime for a broader range of individuals, making it easier for those with limited technical skills to use fully automated bots at scale that cause widespread damage to businesses and consumers.

The CaaS model's affordability and accessibility means that security teams must evolve in parallel to combat the increasingly professional and well-resourced cybercriminals orchestrating these attacks, which is why your bot management strategy should include detection as well as prevention. As CaaS providers offer anonymity, law enforcement faces an uphill battle tracing the origins of these assaults, making it imperative for enterprises to fortify their defenses against this escalating threat.

These two technology trends fuel cybercrime. The purpose of this report is to provide fresh insights – derived from threat intelligence data from the most recognizable companies in the world – to help you derive an incisive understanding of the issue, inspire your strategy, and adapt your tactics.

> "The massive rise of CaaS has completely changed the economics for adversaries. It's much cheaper to attack companies and the attacks are just better because it's a dev shop that is doing the attacks instead of just individual cybercriminals."
>
> – Kevin Gosschalk, founder and CEO, Arkose Labs

## The Contemporary Attack Landscape

We analyzed tens of billions of sessions worldwide across industries, between January 2023 and September 2023, and assessed three primary attack vectors fraudsters use to launch attack types, like SMS toll fraud, scraping, card testing, and more.

**Basic Bots**

Limited bots that perform simple, repetitive tasks

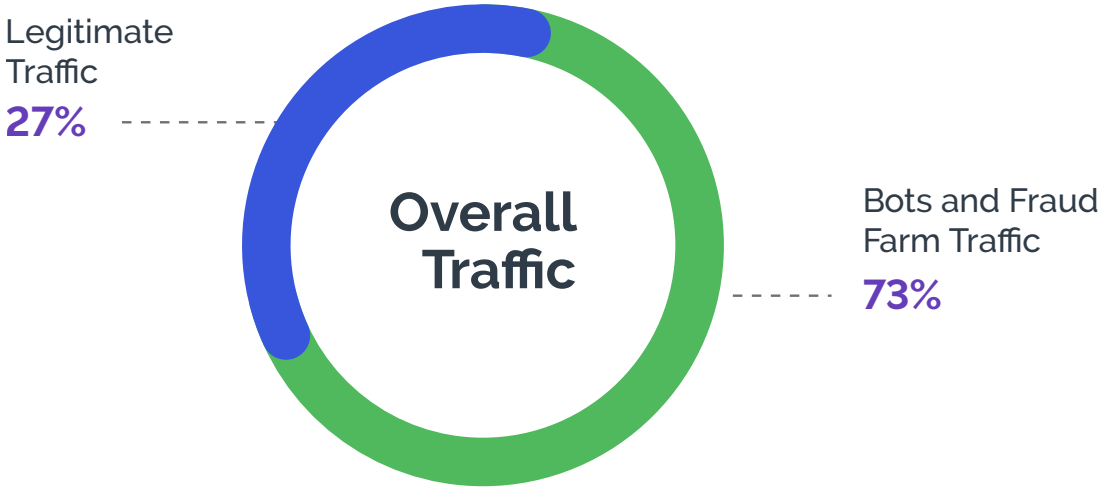
**Intelligent Bots**

Bots capable of complex, context-aware interactions

**Human Fraud Farms**

Organized networks, powered by coerced labor or work-from-home employees in low-wage areas. They leverage solvers that often use automation

Altogether, these attack methods generated **tens of billions of attacks in the first half of 2023 and into Q3,** comprising 73% of website and app traffic measured. In other words, almost ¾ of traffic to digital properties is malicious.

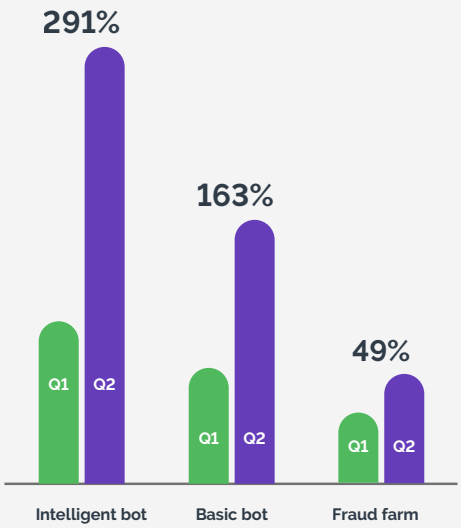



## The Intelligent Bot Uprising

Technological advancements. Financial incentives. Increased resource availability. These are just some of the factors contributing to a growing army of complex, advanced bots. Intelligent ones employ sophisticated techniques like machine learning and AI to mimic human behavior and evade detection. This makes them skilled at adaptation as they target vulnerabilities in IoT devices, cloud services, and other emerging technologies.

From Q1 2023 to Q2 2023, intelligent bot traffic nearly quadrupled—far outpacing basic bots and heavily contributing to a total increase of approximately 167% for all bot attacks.

Increase in Attack Types from Q1 2023 to Q2 2023

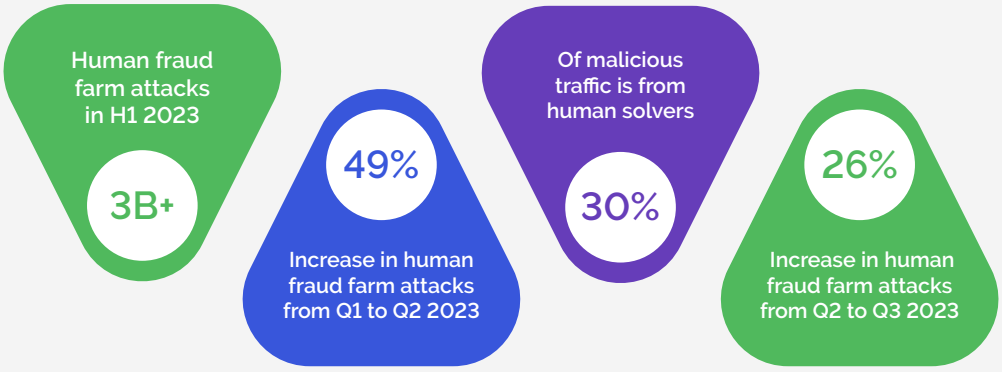


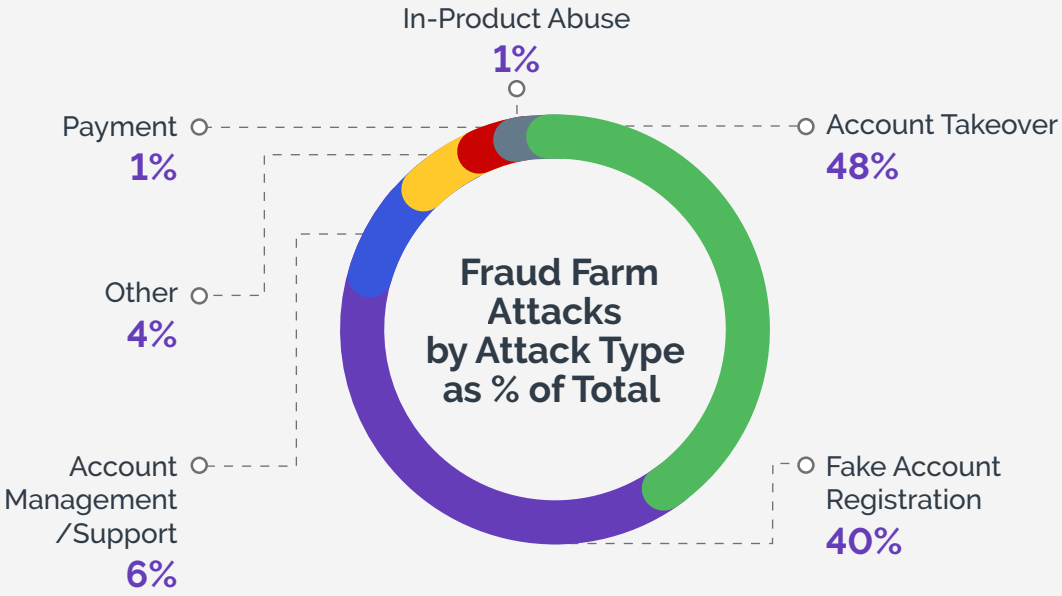
# Human Fraud Farms: Depths of the Underworld

When malicious bots fail to make it past security defenses, bad actors turn to human fraud farms to carry out attacks. Typically operated by organized criminal groups, these attackers are resorting to extreme measures to overcome challenges designed to stop bots. This includes utilizing automation within solvers to rapidly scale their operations. It's important to note, these actions come at a significant human cost, often involving involuntary labor.

**These actions come at a significant human cost, often involving involuntary labor.**

Stopping these adversaries demands technology that dynamically targets human solvers and applies adaptive, time-consuming challenges. With this capability in place, businesses can defeat the economics behind attacks that exploit humans at scale.



# Overall Attacks by Type

Almost across the board, attacks were up significantly from Q1 to Q2 2023.

## Top 5 Attack Types

### Fake Account Creation

Attacks connected with initial registration for an online account

### Account Takeover

Attacks associated with logging into an account, such as ATO and credential stuffing

### Scraping

The scraping of data, content, and images for malicious purposes

### Account Management

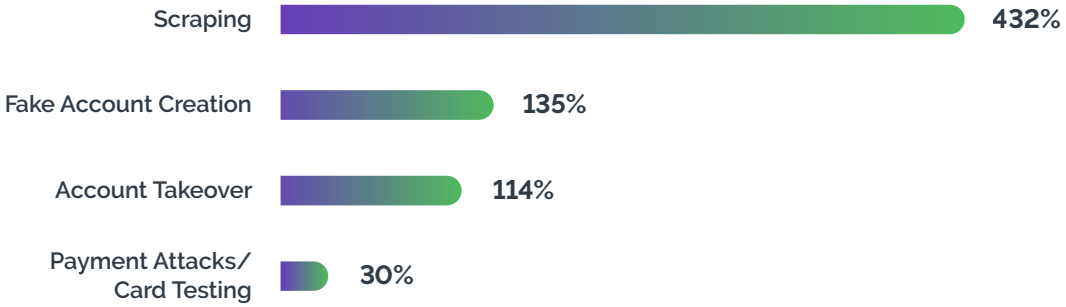
Attacks on customer support call centers, including password resets

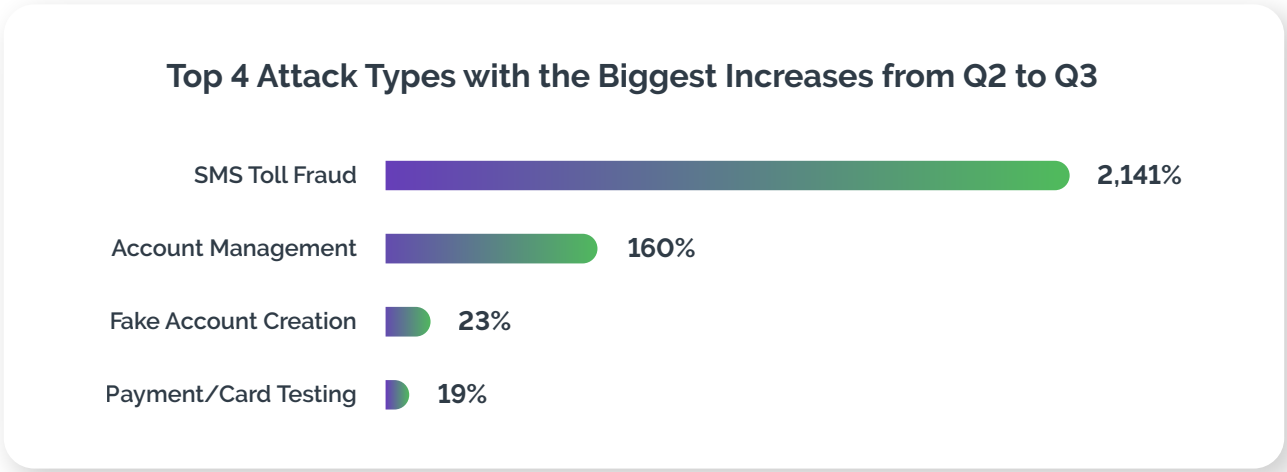
### In-Product Abuse

Abuse including inventory hoarding, loyalty point abuse, chat abuse, bogus gaming sessions, cheating services, and win-loss trading

Top 5 attack types in Q3 were the same as in Q2 with one exception. Instead of in-product abuse, the fifth-ranking attack was payment, which consists of card testing attacks. Cards are a valuable tool, especially around summer holidays and going into the fall holiday shopping season.

### Top 4 Attack Types with Biggest Increases from Q1 to Q2






# A Look Ahead: SMS Toll Fraud

SMS toll fraud attacks, where bad actors create fake accounts at scale that trigger SMS text messages via premium-rate numbers, is one of the most pernicious attack vectors. By the time businesses get the bill and realize they've been scammed, it's too late.

The data indicates a huge surge in this attack type for the second half of 2023.

**Fresh analysis shows that SMS toll fraud was up more than 2,100% in Q3 over Q2 and up 386% over the entire first half of 2023.**

Our data reveals that such attacks are often associated with developing countries, often in Southeast Asia, where the potential for a small profit margin in U.S. dollars can yield substantial gains for the bad actors there. However, there are notable exceptions to this pattern. The U.K., for one, stands out due to its utilization of premium numbers. Unlike some countries with more stringent restrictions, the U.K.'s privatized telecoms sector has left these premium numbers relatively unrestricted, And because the average international SMS cost charged by a leading provider in the U.K. is roughly five times greater than that of the U.S., the U.K. is an attractive target for SMS toll fraud scams.

SMS toll fraud, the stealthy saboteur of business finances, often lurks in the shadows, unnoticed until it's too late. Enterprises send and receive SMS messages as part of the digital identity authentication process, unaware that malicious actors (and sometimes colluding telcos) are inflating their bills. It's a financial ambush. Interestingly, this is a cybercrime that the CFO organization, not the CISO organization, typically detects. Only when businesses receive a shockingly large SMS bill do they realize it was SMS toll fraud. By then, the damage is done—funds drained, resources strained, and reputations at risk.

But SMS toll fraud can be curbed. A prominent gaming retailer successfully identified and halted the issue, preventing over $450,000 in monthly fraudulent SMS charges. Similarly, a leading social media company saved approximately $3 million per month by putting an end to SMS toll fraud.

**Gaming Merchant**

Over
**$450,000**
per month savings in fraudulent SMS charges

**Social Media Company**

Saved
**$3 million**
per month in fraudulent SMS charges

## Industry Benchmarks

Bots and human fraud farms pose multifaceted threats across industries. In the first half of 2023, nearly every industry experienced an increase in the number of attacks. Here are the top 5 industries under attack, by volume.

| RANK #1 | RANK #2 | RANK #3 | RANK #4 | RANK #5 |
|---|---|---|---|---|
| Technology | Gaming | Social Media | Travel and Hospitality | Financial Services |

Early analysis of Q3 data indicates that technology, gaming, social media, and financial services retained their rankings. E-commerce (#4) replaces travel and hospitality in the third quarter.

# Bad Bot Traffic

The percentage of traffic by industry that comes from bad bots.

| | |
|---|---|
| Travel and Hospitality | 76% |
| Technology | 71% |
| Retail | 65% |
| Streaming | 61% |
| Gift Cards | 57% |
| Social Media | 46% |
| Financial Services | 45% |
| Video Gaming | 29% |
| Dating | 21% |
| Security | 20% |

No industry is immune from bad actors, but the specific ways in which they are impacted vary. Here are some common attacks carried out by malicious bots and human fraud farms by industry.

**Travel and hospitality:** Some companies in the travel and hospitality industry engage in inventory hoarding by placing holds on competitors' seats or reservations. They then release them slowly as demand increases, manipulating pricing dynamics and potentially undercutting competitors by offering cheaper rates early on. Scraping has surged this year because of new services built with AI that use bots to scrape at scale (see page 8). In Q3, 72% of attacks in the travel and hospitality industry were web scraping attacks.

**Technology:** The biggest companies in the world fit into this category. Adversaries view them as "high-value" targets because it's lucrative to attack them. Attacks tend to be account takeovers, credential stuffing, fake account creations, and even bonus abuse, which is when adversaries register to take advantage of free trials and sign-up credits. Payment attacks, which include card testing, had an impact on big tech companies throughout 2023, increasing quarter-over-quarter, up 103% in Q2 and then up again a massive 1,034% in Q3.

**Retail/e-commerce:** Online stores are vulnerable to a wide array of scams, especially around the holidays when they want to ensure legitimate consumers can access their goods and services and therefore generally tend to relax their security measures, thinking that the volume of good transactions will outweigh any increase in fraud. In one scenario, bad actors create fake accounts using stolen credit card information and then make fraudulent purchases, resulting in financial losses for the retailer. These days, fraud can no longer be considered a "cost of doing business."

**Streaming services:** Scammers often lure potential consumers by advertising significantly lower subscription prices than the official streaming service providers. These prices may be offered as one-time payments or recurring fees. They also get consumers' credentials, like username and password, from the dark web and then sell them to other consumers, instructing those buyers not to change the credentials.

**Gift cards:** Attackers steal revenue from gift card companies in multiple ways. In one common scenario, a scammer convinces a victim to share the card details or codes of gift cards they have purchased. The scammer then exploits these details to steal the card's value, leaving the victim with financial losses and no way to recover their money. Gift card fraud tends to increase around the holidays, in part because bad actors hope to hide within the extremely high volume of gift card purchases to perpetuate this scam.

**Social media:** Fraudsters create fake accounts to seem more credible and attract more followers. They use these accounts to trick real users, build trust, and spread their own messages or influence others, sometimes even affecting elections. They also scrape data, content, and images, using this treasure trove of information for malicious purposes like identity theft or social engineering schemes. Social media scraping attacks rose 11% in the second quarter.

**Financial services:** Banks, fintechs, and insurance companies are the most lucrative targets for attacks. Account takeover (ATO) attacks have become increasingly prevalent in the banking industry, accounting for one out of two attack attempts observed by our team in Q1 2023. Throughout 2023, fake account registrations have steadily increased. In the third quarter, these attacks jumped 30% over Q2.

**Video gaming:** Fake account creation drains video gaming companies and their customers of millions of dollars in multiple ways. To name just a few, bad actors can manipulate the in-game economy by taking over items and selling them at a premium, level up account profiles that can then be sold off to other gamers, or rake in virtual currency through in-game botting, which can trigger thousands of matches automatically. Gaming companies experienced a 69% spike in fake accounts in Q2 over Q1, but this attack seems to have leveled off, essentially remaining flat with a 1% increase in Q3 over Q2. Every quarter, payment attacks (which include card testing) have been escalating with a 29% increase in Q2 over Q1 and a 15% increase in Q3 over Q2. An attack gaming companies might not expect is account management, wherein fraudsters try to change passwords, and other administrative tasks. Account management attacks leapt 313% in Q2 over the first quarter and then leapt again 61% in Q3 over Q2.

**Dating services:** In particularly insidious attacks, bad actors create fake accounts so that they can conduct sex and labor trafficking recruitment. Human trafficking is a very lucrative crime, reaching $150 billion in profit. As mentioned earlier, our threat researchers observed a more than 36,000% increase in fake account creations in Q3 over Q2. They also noted a 4,992% increase in bot attacks – both intelligent and basic bots – on dating sites in Q3 over the second quarter.

**Security:** Bots attempt account takeovers at security companies for reasons including data theft, financial gain, competitive advantage, espionage, and resource hijacking, among other motivations.

# The Growing Scourge of Attacks

| Industry | Increase in Overall Attacks from Q1 to Q2 | Increase in Bot Attacks from Q1 to Q2 | Increase in Human Fraud Farm Attacks from Q1 to Q2 |
|---|---|---|---|
| Travel and Hospitality | 1270% | 1515% | 310% |
| Streaming | 316% | 334% | 57% |
| Social Media | 109% | 216% | 16% |
| Financial Services | 159% | 156% | 355% |
| Video Gaming | 96% | 152% | 60% |
| Retail and E-commerce | 44% | 72% | 2% |
| Technology | 133% | 152% | 60% |
| Gift Card | -36% | -48% | 47% |

## Spotlight on Credential Stuffing

ATO attacks are the top attack type for most industries, including dating, financial, gaming, media, and security.

Credential stuffing, a common type of ATO attack where bad actors use stolen usernames and passwords from one website to gain unauthorized access to another, exploits the fact that many people reuse credentials across multiple platforms.

**ATO attacks more than doubled from Q1 to Q2 2023, with a 106% increase**

Attacker

Collection of stolen login credentials

Bots

Victim Service

# Attack Type Breakdown by Industry in H1 2023

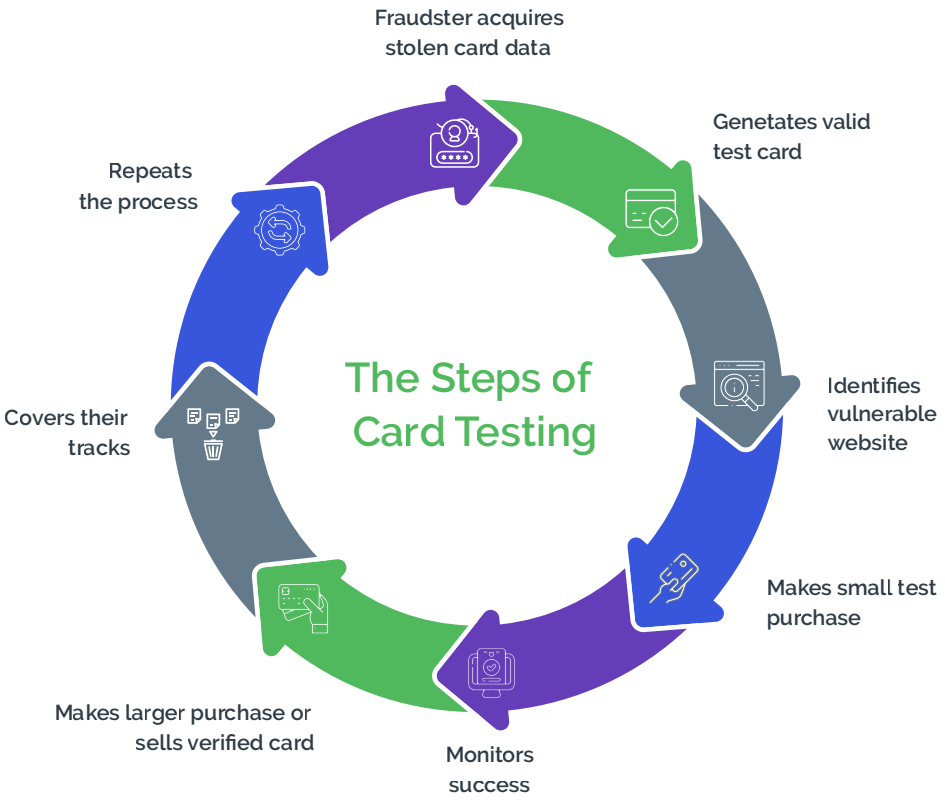
| | Account Takeover (ATO) | Fake Account Regisitration | ATO + Fake Account Registration | Payment Abuse | In-Product Abuse | SMS Toll Fraud | Account Management Attacks | Scraping |
|---|---|---|---|---|---|---|---|---|
| Dating | #1 | #2 | | | | | | |
| Financial Services | #1 | #2 | #3 | #4 | | | | |
| Video Gaming | #1 | #2 | | #3 | #4 | | #5 | |
| Gift Cards | #1 | | #2 | | | | | |
| Streaming | #1 | | #2 | | | #3 | #4 | |
| Retail and E-commerce | #3 | #1 | #4 | | | | #2 | |
| Security | #1 | | | | | | | |
| Social Media | #2 | #1 | | | #5 | | #4 | #3 |
| Technology | #2 | #1 | | #4 | | | #3 | |
| Travel and Hospitality | #2 | #3 | | | #5 | | #4 | #1 |

# Spotlight on Card Testing

An age-old menace has resurfaced. In card testing attacks, fraudsters attempt to validate stolen credit card information by making small purchases and/or testing card details on websites.

Card testing, or carding, is a silent predator. Bad actors exploit the online shopping ecosystem by methodically testing stolen credit card information on merchant websites. Their actions often go undetected until a sudden surge of failed transactions and chargebacks wreaks havoc on businesses. In real life, card testing involves criminals using automated scripts or manual methods to input multiple stolen credit card numbers, probing for vulnerabilities in payment systems. As they discreetly verify card details, organizations remain unaware of the looming danger. As businesses strengthen their digital defenses against these hidden adversaries, they protect their financial integrity and customer loyalty from the insidious impacts of card testing.

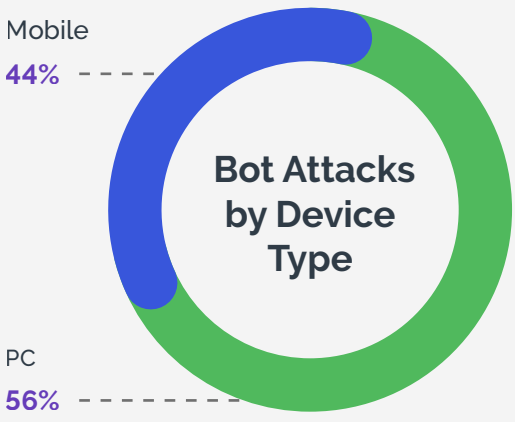
**From Q1 to Q2, payment attacks, which include card testing, were up 30%.**




# Bots on the Move

As mobile usage grows, so too does the proliferation of bot attacks via mobile devices. Mobile attacks often originate from regions where mobile devices are more widespread than laptops, creating large segments of the population with smartphones but no laptops. The uniformity in mobile device usage also provides attackers with a cloak to hide among genuine users.


Mobile Attack Increases from Q1 2023 to Q2 2023



# Top 5 Mobile Attack Types

### Fake Account Creation

Attacks connected with initial registration for an online account

### Account Takeover

Attacks associated with logging into an account, such as ATO and credential stuffing

### Account Management

Attacks on customer support call centers, including password resets

### In-product abuse

Abuse including inventory hoarding, loyalty point abuse, chat abuse, bogus gaming sessions, cheating services, and win-loss trading

### Payment Attacks

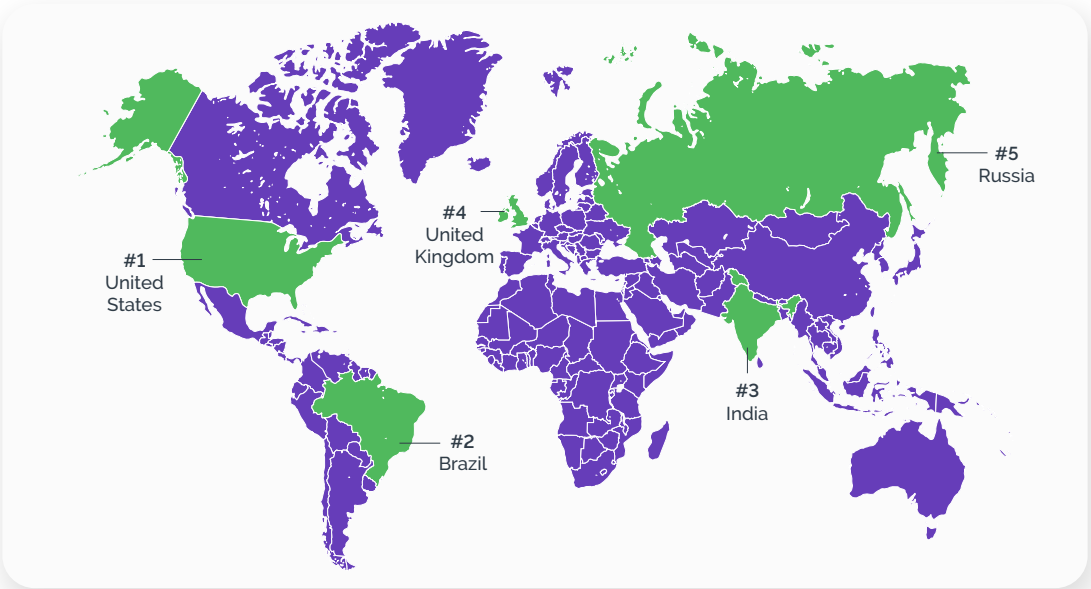
The use of stolen payment information for unauthorized digital transactions, including card testing payments

## The Worldwide Assault Terrain

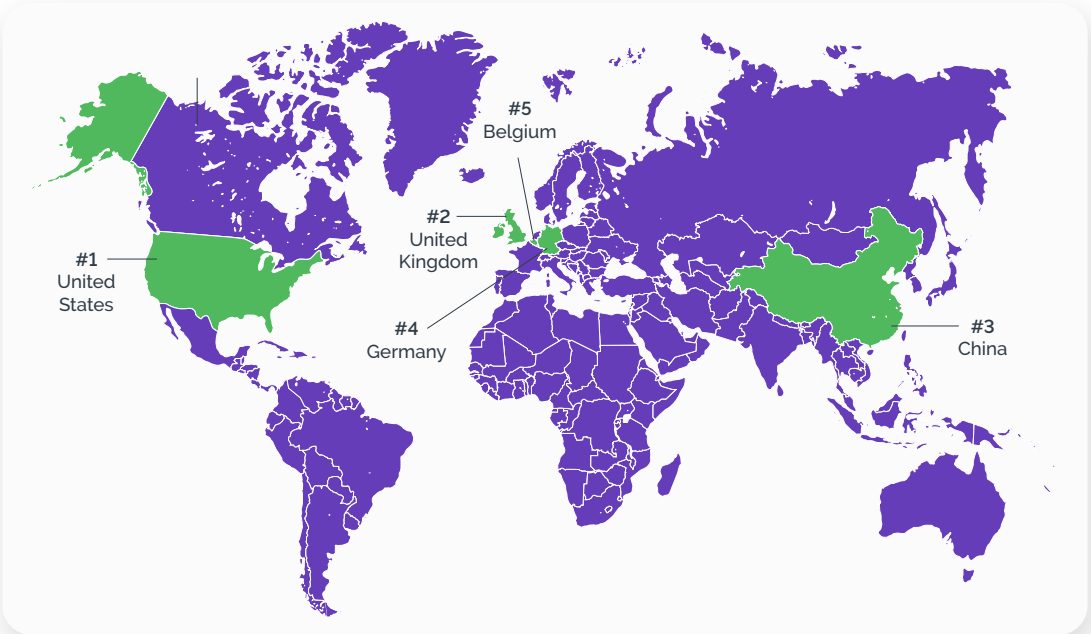
Where are these cyberattacks coming from? Cybercriminals are concealing their identities by operating from countries with strong credibility and well-established data center infrastructures. This tactic allows them to evade cybersecurity defenses, complicating companies' efforts to implement geographic-based control strategies as they aim to avoid blanket blocking of entire countries.

But security pros need to know the geographies being used in these masked campaigns so they can regularly tune their control strategies.

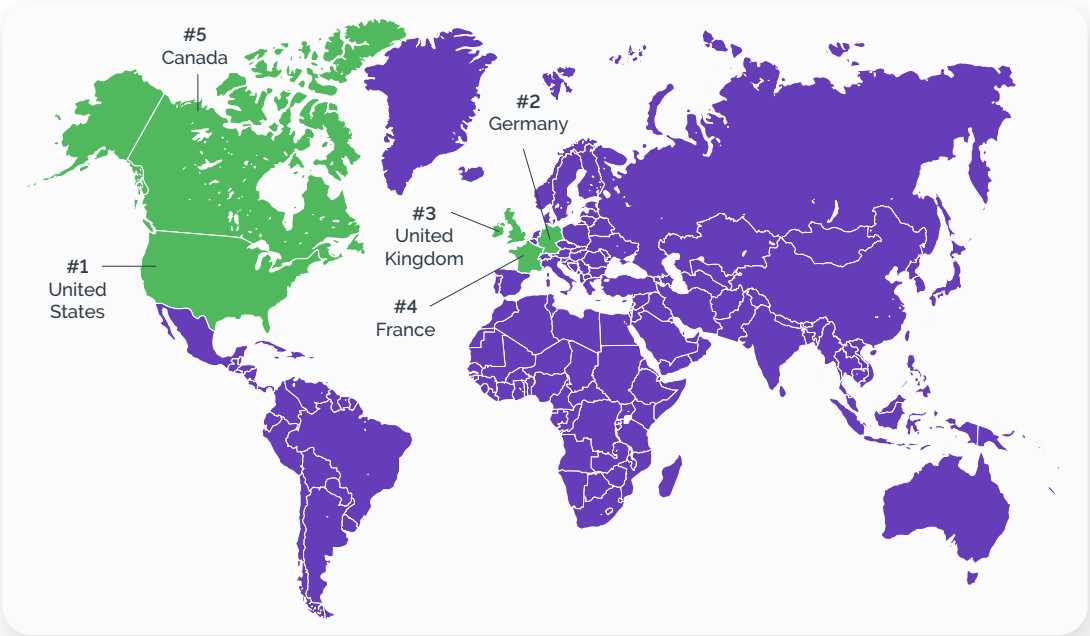
## All Attacks: Top 5 Countries of Apparent Origination



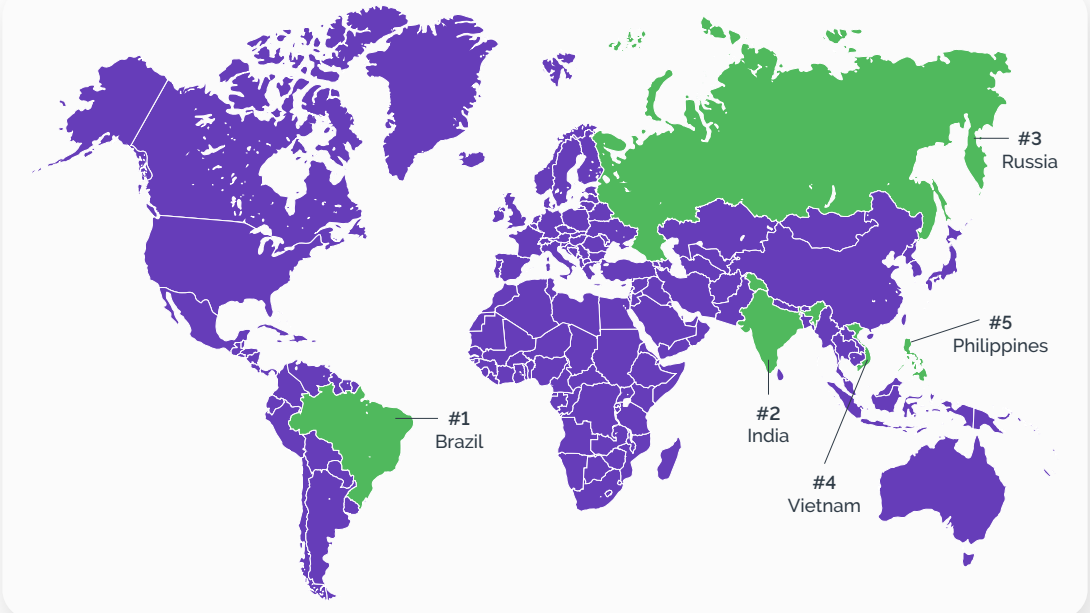

## All Bot Attacks: Top 5 Countries of Apparent Origination



## Intelligent Bot Attacks:
## Top 5 Countries of Apparent Origination

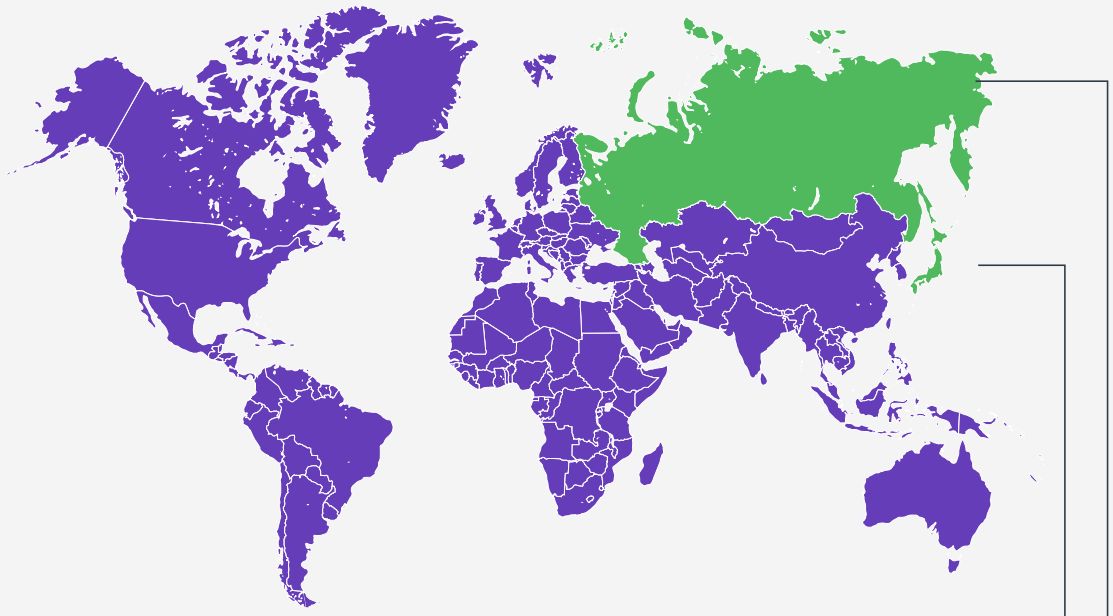



## Fraud Farm Attacks:
## Top 5 Countries of Apparent Origination



# Notable Attack Vectors by Region

Bots fuel a variety of attack types worldwide. Two that stand out in H1 2023: SMS toll fraud and account management, which consists primarily of password resets.



**Russia:**

Apparent origination of the most account management/support attacks. Russia appears to be the primary source of account management/support attacks, with evidence pointing to the presence of larger, well-known adversaries operating in this region. This suggests that the perpetrators may not be actively concealing their locations but rather operating openly.

**Japan:**

Apparent origination of the most SMS toll fraud attacks. With its abundant premium numbers and robust data infrastructure, Japan is a likely origin for SMS toll fraud attacks. But bad actors also leverage Japan's reputation as a low-risk country to mask where attacks truly originate so they can increase the likelihood of success.

## Microcosm of H1 2023: The week of May 7, 2023

For the week of May 7—the week with the highest overall attacks during Q1 and Q2—ATO attacks made up 47% of all attacks.

- 75% of the attacks for the week of May 7 were conducted by bots.
- 25% of the attacks for the week of May 7 were conducted by human fraud farms.
- The industry most attacked was gaming, followed by technology and then travel.
- In the gaming industry that week, 92% of the attacks were ATO, 65% of which were conducted by basic bots.

The week of May 7 was a big one for gaming in 2023 with the highly anticipated release of The Legend of Zelda: Tears of the Kingdom bringing attention to the gaming world. People flocked not just to that game but to other launches as well. The week prior had seen the launches of Redfall and Age of Wonders 4. Mobile games launched the week of May 7 included EA's Lord of the Rings: Heroes of Middle Earth.

# How Arkose Labs Can Help

Financial incentive is what fuels bot attacks. Arkose Labs delivers long-term bot mitigation and account security by undermining the economic drivers behind attacks. We help global companies defend the most targeted user touch-points – account login and account registration – by uncovering hidden attack signals and sabotaging attackers' ROI without sacrificing good user throughput.

We protect businesses from evolving attacks, block automated activity aimed at monetizing stolen data, and secure the consumer experience. Arkose Labs' unique bot detection and mitigation platform, Arkose Bot Manager, analyzes data from user sessions to determine the context, behavior, and past reputation of every request. We classify traffic based on its risk profile and present suspicious traffic with enforcement challenges to differentiate between legitimate users and fraudsters.

$Millions Saved in Costs Associated with Fraud Attacks

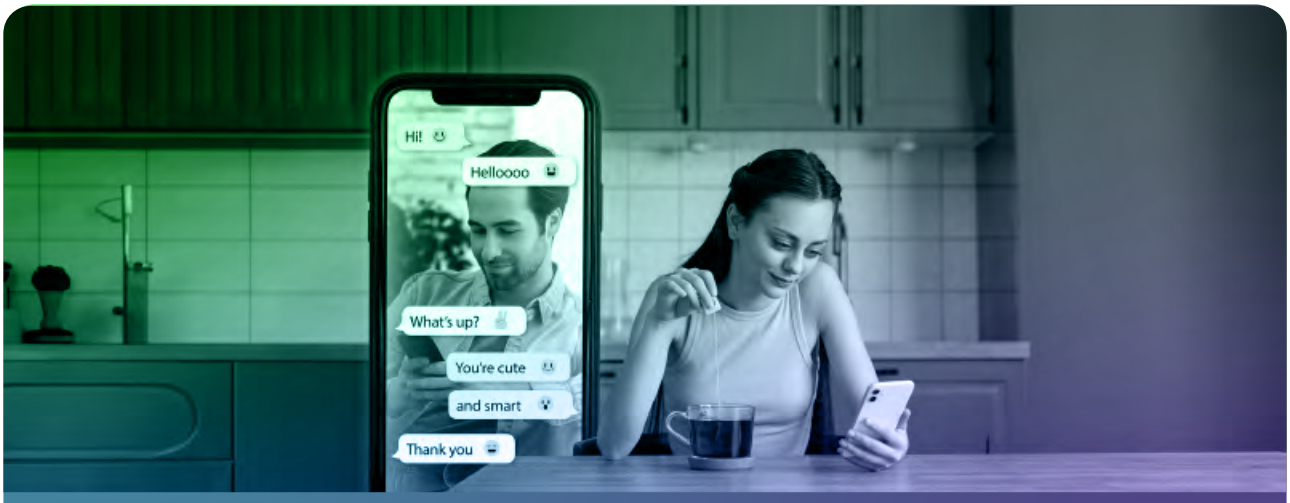
80% Reduction in Good User Friction

98% Reduction in Bot Attacks


## Fast-Growing Neobank Faces Off Against Credential Stuffing

Bots were relentlessly targeting a leading neobank's user accounts for credential stuffing, resulting in drained customer accounts and a deteriorating user experience. The financial services company implemented Arkose Labs to protect its log-in forms and back-end APIs. This implementation led to remarkable results, including:

- 75% decrease in account takeover (ATO) attempts
- Slashed compromised account costs, which previously hit $100,000 per week
- Unleashed efficiencies through reduction in customer support demands




## Global Dating Platform Battles Phony Accounts

Fraudulent new account creations were plaguing a global dating site, where malicious individuals were likely making attempts to engage in profitable romance scams or potentially more sinister activities like human trafficking. The platform adopted Arkose Labs solutions to identify and crush cyberattacks, ultimately protecting the dating company and its client base:

- 80% reduction in fake account registrations
- Put the brakes on downstream spam and abuse
- Safeguarded interests of genuine customers

# Arkose Labs

The mission of Arkose Labs is to create an online environment where all consumers are protected from spam and abuse. Recognized by G2 as the 2023 Leader in Bot Detection and Mitigation, with a high score in customer satisfaction and the largest market presence six quarters running, Arkose Labs offers the world's first $1M warranties for credential stuffing, SMS toll fraud, and card testing. With 20% of our customers being Fortune 500 companies, our AI-powered platform combines powerful risk assessments with dynamic threat response to undermine the strategy of attack, all while improving good user throughput. Headquartered in San Mateo, CA, with offices in Argentina, Australia, Costa Rica, India, and the U.K., Arkose Labs protects enterprises from cybercrime and abuse. For daily insights pertinent to the shifting threat landscape, follow the company on LinkedIn.


**Sales:**

(800) 604-3319

**Mail:**

connect@arkoselabs.com

**Address:**

U.S. • 400 Concar Dr., San Mateo, CA. 94402

Australia • 310 Edward Street, Brisbane QLD 4000

U.K. • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF

Costa Rica • Calle 118B San Rafael, San José, SJ 1020

India • Redbrick Offices, Tower B, Panchshil Business Park, Pune, Maharashtra 411045

Argentina • Avenida Corrientes 800, Buenos Aires, Buenos Aires C1008


Schedule Demo