Arkose Labs

# Q1 2021
# FRAUD AND ABUSE REPORT

*Insights from the Arkose Labs global network*

# Introduction

I think it's safe to say we are all happy to turn the page from 2020 into a new calendar year. We're all hoping that life returns to normal in many ways as we move on through 2021, but one thing that likely won't change is a return to pre-pandemic digital traffic and fraud levels.

2020 saw an unprecedented spike in digital traffic as homebound people around the world went online for shopping, entertainment, education, socializing and remote work. For some it was their first foray online, and a new segment we call "digital debutants" was born.

This led to an increase in attacks as fraudsters attempted to blend in with good users. With more people online at all hours of the day, typical models of what good and bad behavior looked like were thrown out the window. Credential stuffing attacks were a major attack vector in 2020, as fraudsters attempted to hack into accounts at scale in order to commit downstream fraud.

No one knows what the rest of 2021 holds, but it's imperative we all work together to stamp out fraud and make the digital world a safer place for all.

Though we may be turning the page on 2020, one thing that is certain is that the frequency and severity of fraud attacks will never go back to pre-pandemic levels.

**Kevin Gosschalk**

Founder and CEO

As the world is more digital and economic turmoil  continues, heightened attack levels are here to stay. Businesses need long-term strategies to defend against high velocity fraud and abuse.

# 2020 In Review: Mass Digitalization Spurs on Fraud

**470 million**
SWEATSHOP ATTACKS

**3.9 billion**
BOT ATTACKS

**4.9 billion**
TOTAL ATTACKS

**14.8 billion**
TOTAL TRANSACTIONS

**23%**
ATTACK RATE

**11%**
HUMAN ATTACKS VS BOTS

**17.5%**
MOBILE ATTACK RATE
VS DESKTOP

# What Changed in 2020?

**The Digitized World**
With much of the world stuck inside for large parts of the year, people turned to digital channels for everything from shopping to gaming to streaming media and more. In fact, the Arkose Labs network saw 4 times as many transactions overall compared to the prior year.

**The Changing Face Of Fraud**
As noted earlier, socio-economic factors brought on by Covid-19 forced many typically law-abiding citizens into fraud to make ends meet. There was also an onslaught of chargebacks, as consumers canceled trips and demanded refunds for orders taking too long to ship.

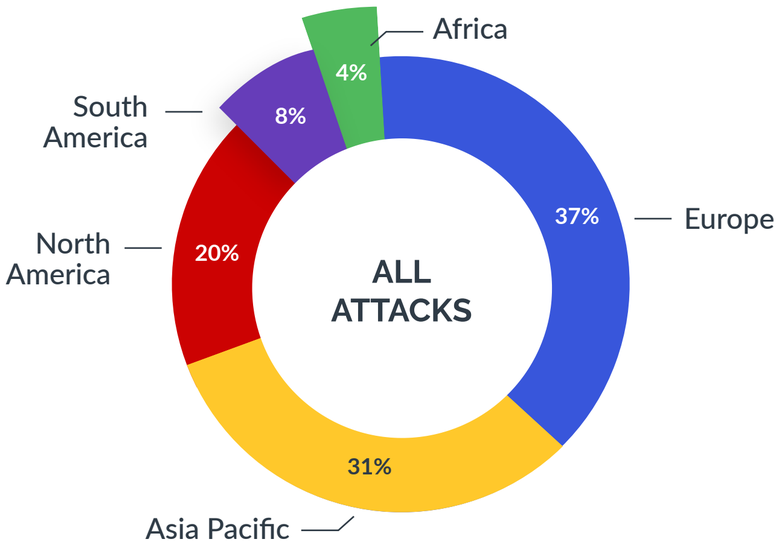
**A Stress Test Of Fraud Systems**
The massive spike in digital traffic to online platforms, made for something of an unexpected stress test for fraud systems. Suddenly, old models of what suspicious behavior looked like were thrown out the window, and for many platforms daily traffic was at rates normally only reserved for the business times of year.

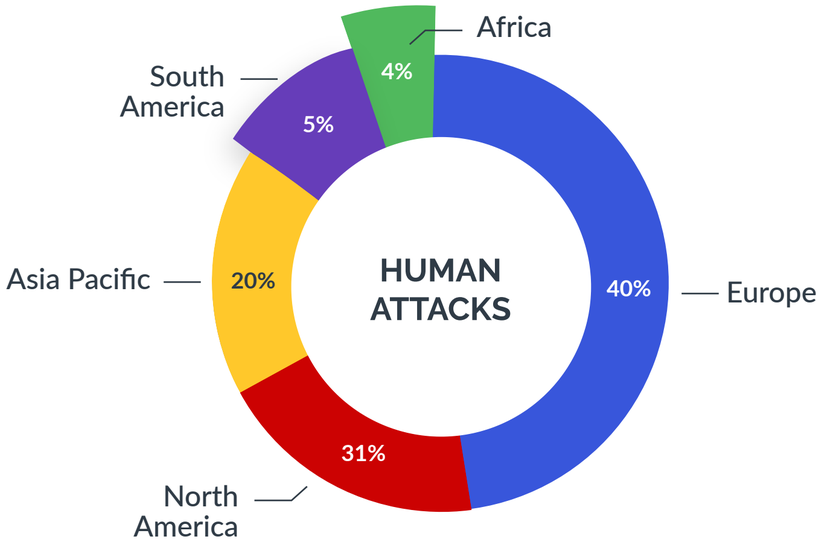
**The New Home Office**
The switch to remote working spurred a much-needed digital transformation for internal fraud and security teams. Many realized that large teams were no longer required to be on-site, and servers could be monitored and even power switches turned on and off remotely.

**New Attack Types**
2020 saw a rise in hybrid attacks, as bots were used to launch many large scale/low reward attacks that relied on brute force, with humans supplementing attacks in which more nuance was required. Account takeover attacks in particular spiked, as fraudsters targeted the wealth of new accounts created by consumers using digital services for the first time.

# 2020 Attacks By Region

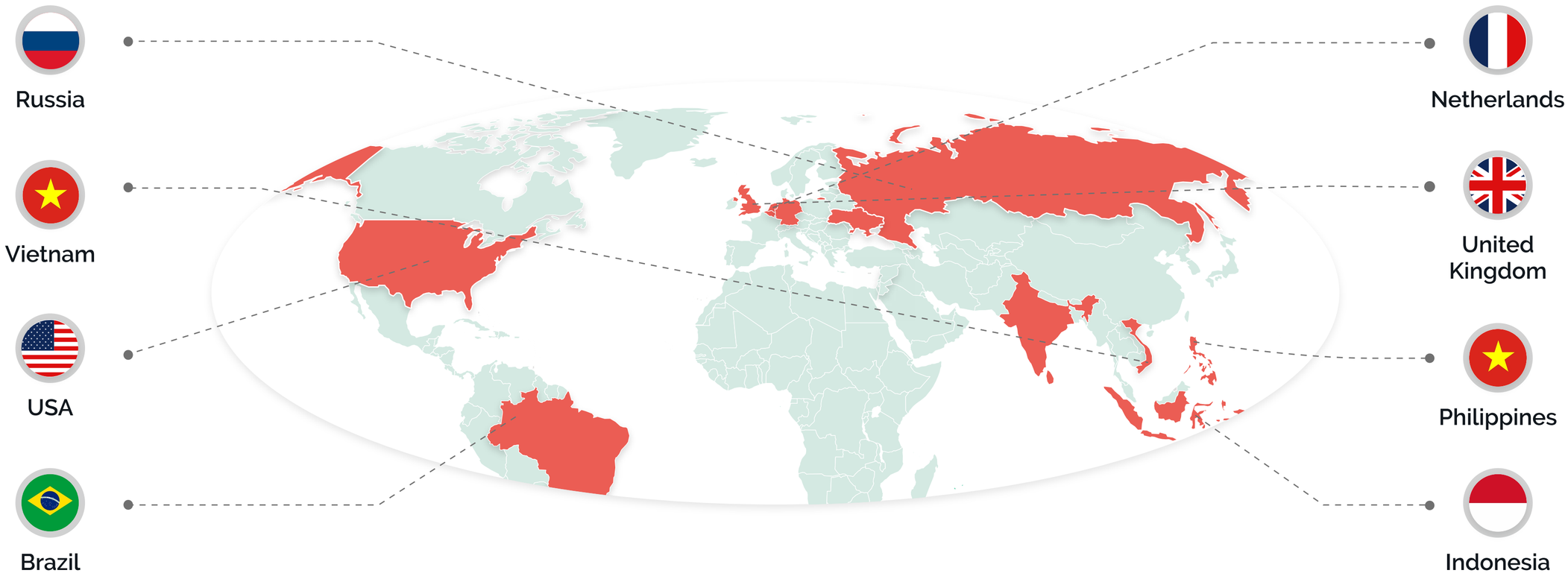
2020 saw a marked change in the geographies where fraud attacks originate from. Typically, the majority of attacks are launched from countries with developing economies, where employment opportunities may be limited. These are typically fertile grounds for fraudsters to recruit from. However, as the Covid-19 pandemic pushed millions around the world into financial despair, many resorted to fraud out of desperation to make ends meet. Europe  emerged as the top overall region for attacks followed by Asia - which was traditionally a more active fraud hub. North America also saw an increase in fraud attacks, specifically from the United States. A great deal of attacks from Europe originated from Russia, along with a spike in malicious activity from major economies in Western Europe.



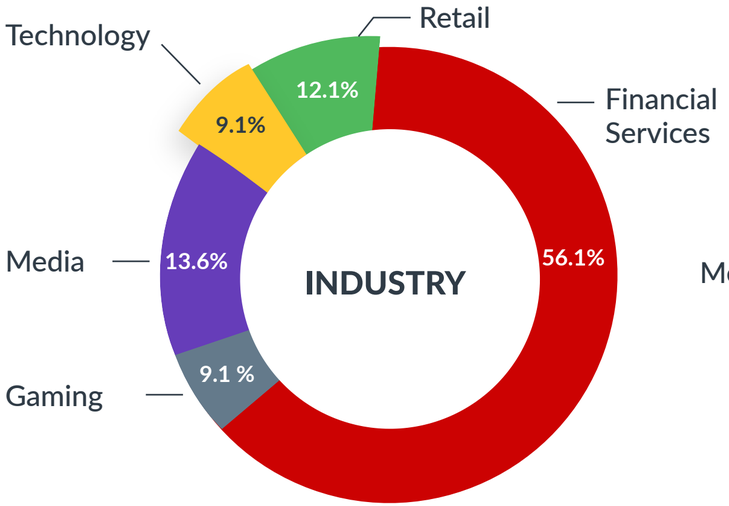
# 2020 Attacks By Country

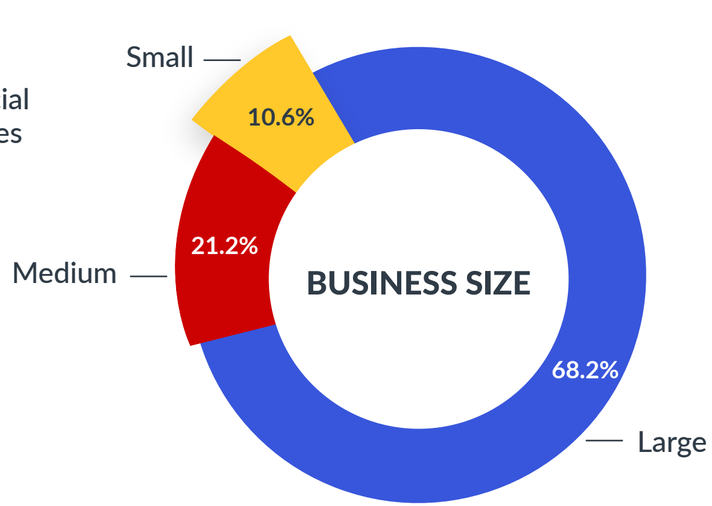
The top attacking countries in 2020 are dispersed across North America, South America, Europe, and Asia, highlighting the truly global nature of the cybercrime ecosystem. The United States featured due to the sheer volume of digital activity here, and the fact that major ecommerce and banking platforms are the top target for many. Traditional fraud hubs in Southeast Asia featured, as well as the more surprising addition of the Netherlands. This was due to a prominent botnet operating from the Netherlands which was being utilized by multiple fraud operations.

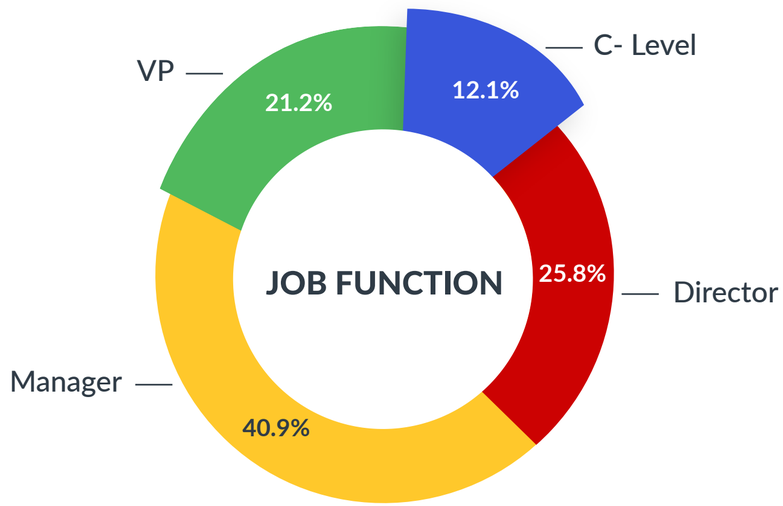


# 2020 End of the Year Survey - Fraud & Security Execs

Arkose Labs assembled 80 fraud and security execs at the end of 2020 to reflect on the key changes from 2020, the biggest winners and losers in the post-Covid digital economy, and the most interesting emerging incidents they have seen. Industry experts came predominantly from large enterprise, including Visa, PayPal, Amazon, eBay, Twitter, Sony, LinkedIn, US Bank, Dropbox, Gap, McDonalds, Capital One, and more.



# 2020 End of the Year Survey: Insights from the Field

### Stimulus Fraud

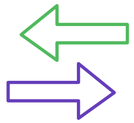
Stimulus checks provided a new way to make instant cash, with an influx of fake or stolen identities were created to open new fake accounts and gain unemployment checks.

### Friendly Fraud

There was an alarming increase in the amount of friendly fraud, with people disputing genuine transactions, fueling a spate of more organized refund fraud attempts.

### Human Click-Farms

There was a spike in human click-farms, as jobless people and those stuck to their homes looked for opportunities to earn money, regardless of where it came from.



### New Avenues

As the number of new digital users swelled, fraudsters found a larger window of opportunity. From price gouging to delivery scams—especially masks and sanitizers—fraud rings milked every opportunity to monetize attacks.

### Phishing & Social Engineering

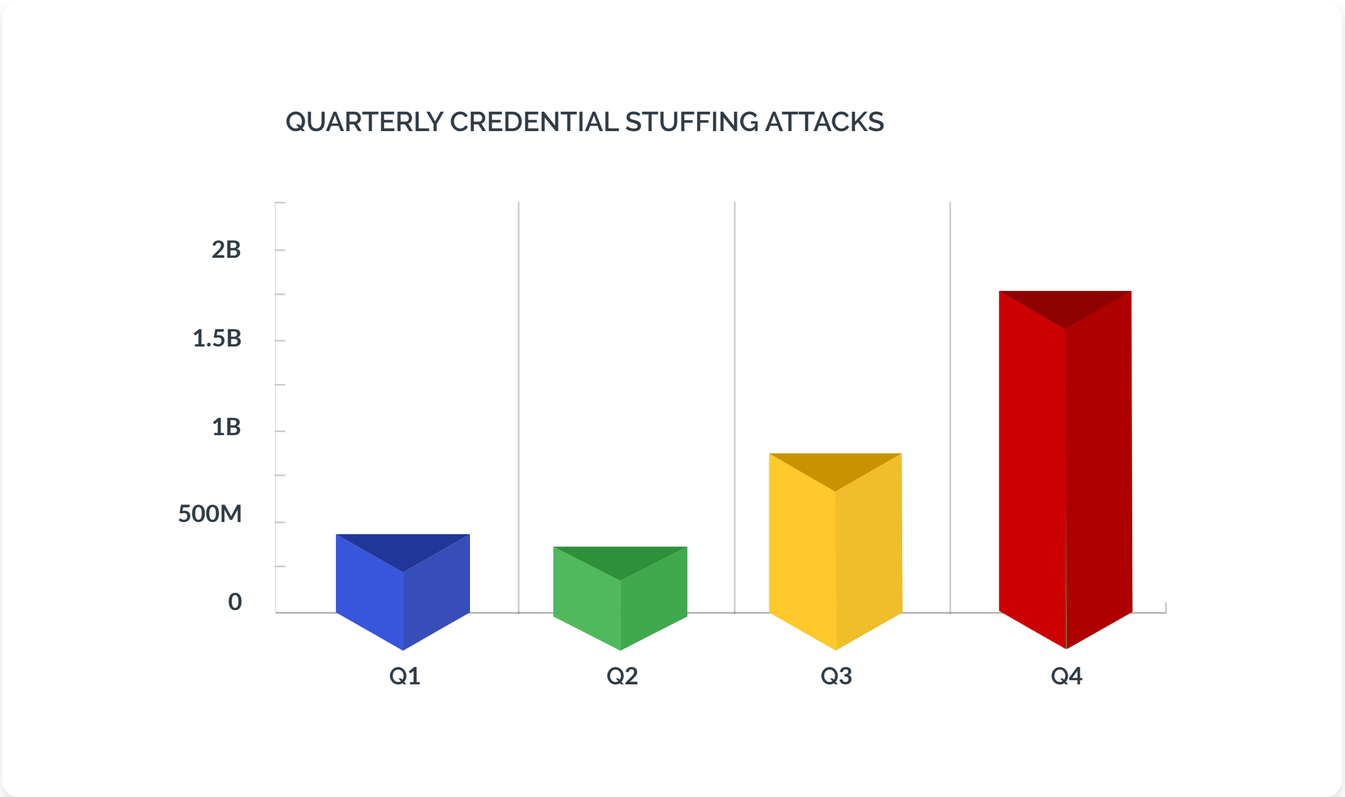
Fraudsters used spam, social media, and social engineering techniques to play on the panic around COVID-19 to trick users into sharing their passwords. They even targeted labs creating vaccines for COVID-19 with ransomware.

### Synthetic Identity

The shift to cash to CNP caused businesses to relook at authorization, fraud models and how to manage identities, especially in the wake of fraudsters increasingly using synthetic identities.

# Explosion in Credential Stuffing Attacks 2H 2020

The influx of new digital accounts created led to a drastic increase in credential stuffing attacks, which powers account takeovers. Account takeover attacks are the fuel that powers fraud; once an account is compromised an attacker can use it to carry out numerous types of downstream fraud. Credential stuffing attacks more than doubled in Q4 compared to Q3, and were around 90% increased from the Q1, before lockdowns came about. It's clear that protecting consumer accounts is vital for digital businesses.



# Love in the Time of Coronavirus: Online Dating in 2020

**4 Million**
Attacks

**8.7%**
Attacks

**22.1%**
Human Driven Attacks

Of all industries, online dating was among those turned upside down the most during pandemic-related lockdowns. Dating apps have exploded in popularity because they allow people to quickly connect in an intuitive and seamless interface. But in 2020, those digital connections didn't lead to drinks, dinner or movies, but rather virtual dates. And many single people, who relied on going out to meet others, turned to dating apps as a way to connect during a solitary time.

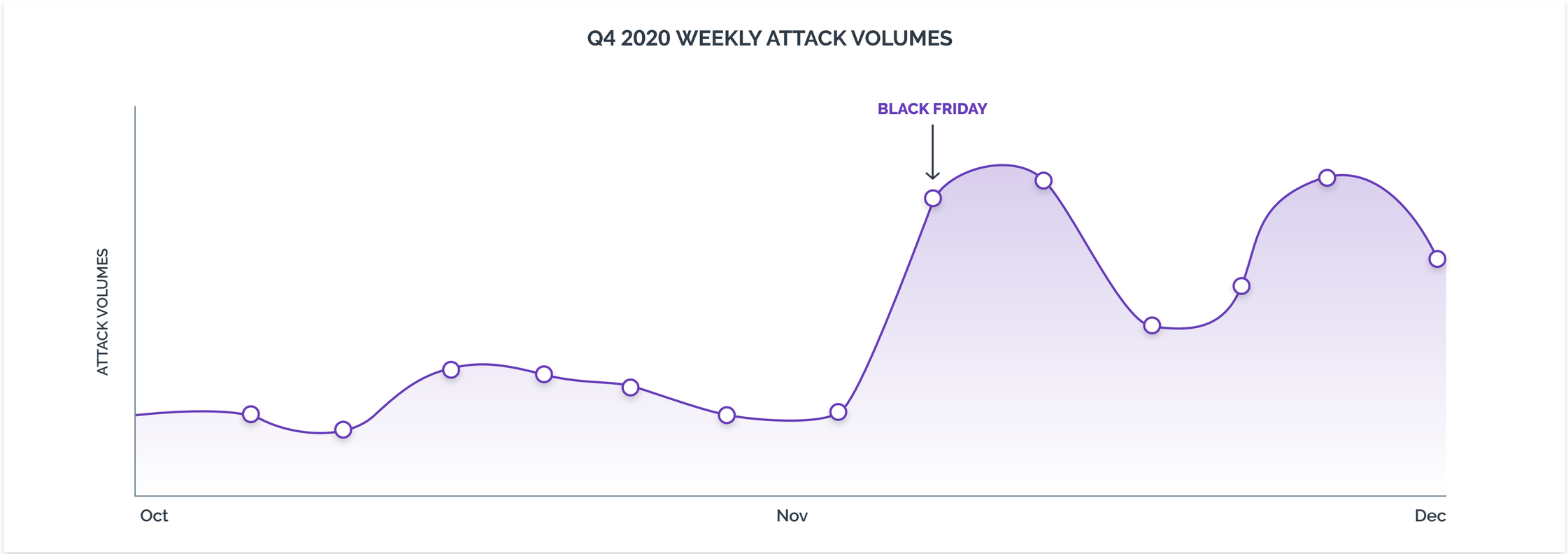
Fraudsters took advantage of this, and targeted dating apps to create fake profiles and scam real users. In 2020, Arkose Labs recorded 4 million attacks targeting dating apps, with an 8.7% attack rate. Nearly a quarter of these were human-driven attacks; such as fraudsters connecting with users and exchanging a few messages messages before asking for money, or by sending messages with links to spam or malicious software. Fraudsters heavily relied on sweatshops to carry out these attacks, as writing and responding to messages required more nuance than off-the-shelf bots could accomplish.

That's a big reason why human-driven attacks are higher in dating than the cross-industry average. Bots were also used to create and open new accounts at scale to commit downstream fraud. All in all, dating apps were a popular target for fraudsters due to the high potential monetization from a scam.

Since the vast majority of attacks in this industry start with fake new accounts registrations, it means that if dating apps and websites can stamp out this type of fraud from the start they can ultimately prevent much downstream abuse and create a safer environment for their good users to find love and romance.

# Heightened Attack Volumes in the Second Half of Q4

Attack volumes in 2020 showed a marked increase from Black Friday onwards. The holiday shopping period is always a hotbed for fraud attacks. However, it is interesting to note that this trend extended beyond industries that are typically involved in the digital commerce splurge at the end of the year, with sharp attack spikes also seen in finance, media, and technology in the second half of Q4 2020. Automation powered the vast majority of attacks, with the attack rate hovering above 25% for much of the quarter.



# The Black Friday Effect: Attacks Up No Matter the Industry

Black Friday is known to be a day where ecommerce sites see a massive spike in consumer traffic --as well as fraud.  This year was no different, as the Arkose Labs network recorded a sustained increase in fraud activity from Black Friday on through the end of the year.

What was different this year was that this same trend was seen through all industries beyond just retail. In some, such as gaming, this was expected since companies in that industry too offered deals and promotions around Black Friday. But industries not typically associated with Black Friday, such as social media platforms, online dating companies and financial services also saw an increase in attacks over the holiday shopping period.

This could be due to fraudsters using things like social media or cloud-based communications platforms to spread disinformation about deals, or simply attacking payments platforms or financial accounts knowing they could blend in with the increased traffic on these sites due to increased consumer usage.

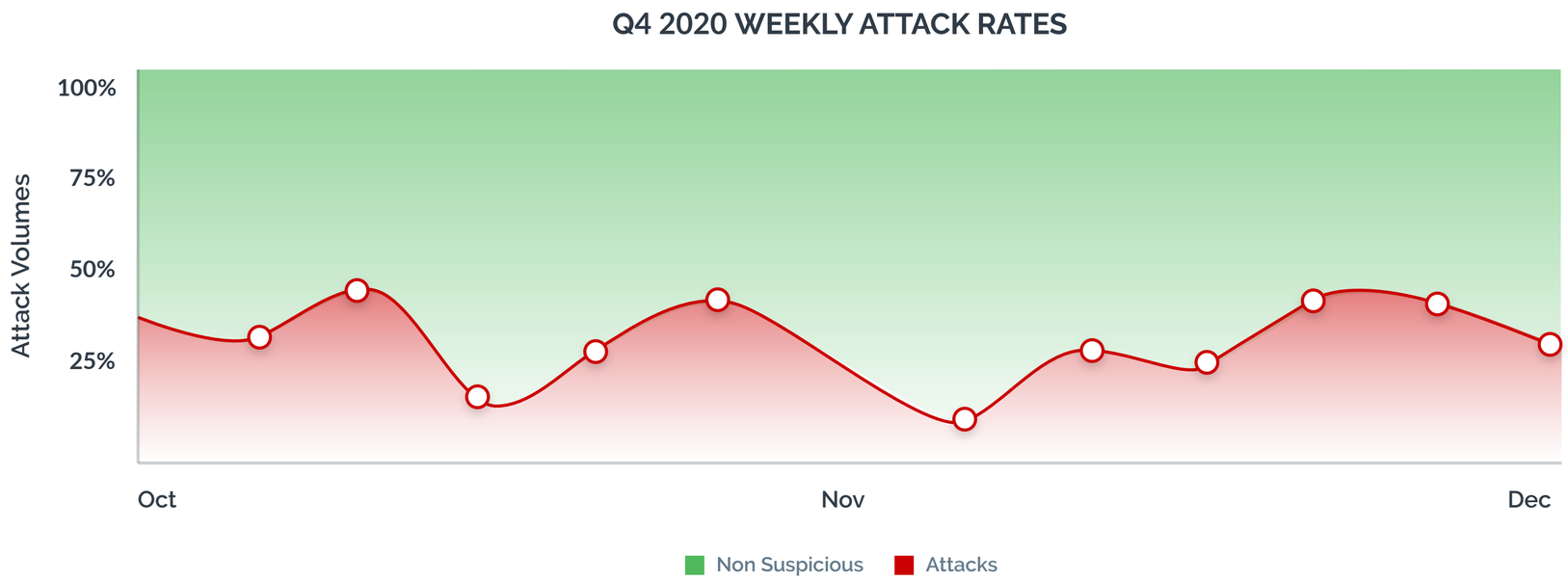
# Q4 2020 Attack Trends

**2.1 Billion**
Attacks

**30%**
Average Attack Rate

**16%**
Mobile Attack Rate

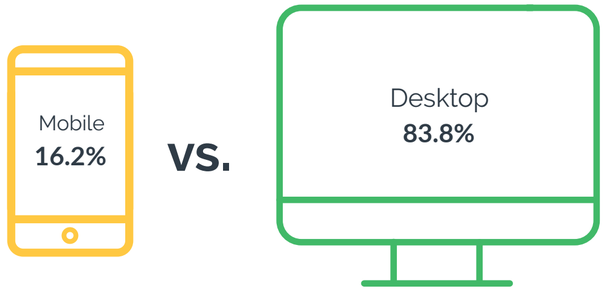
As in previous quarters, bots powered a large percentage of the fraud attacks during Q4, with humans largely being used to supplement hybrid attacks. The average attack rate was nearly 30%, slightly up from the 25% average attack rate seen in Q3 on the Arkose Labs Network. The mobile attack rate rose slightly to 16%. As expected, many industries dealt with an increased spike in attacks during Black Friday. However, as the amount of legitimate transactions also rose greatly during that period, Black Friday did not actually see the peak attack rate for Q4.



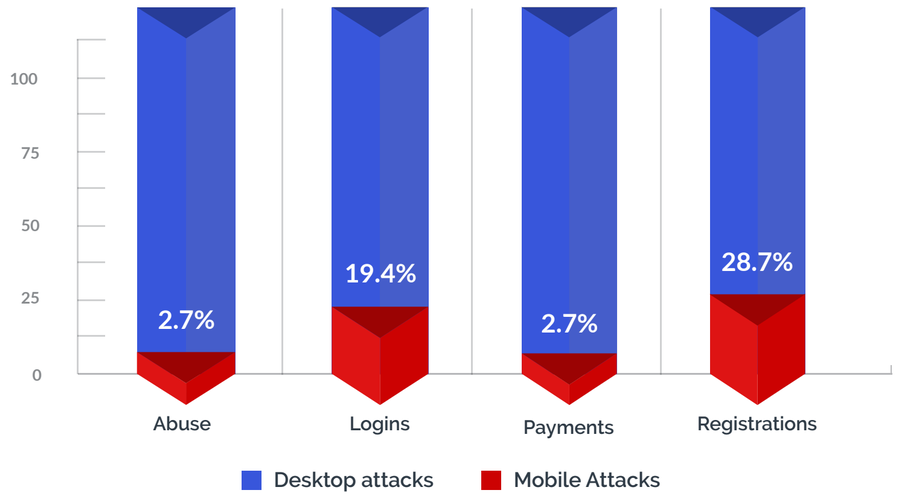
# Rise in Mobile Attack Rates in Q4 2020

There was a rise in the proportion of all attacks that were on mobile transactions versus desktop in Q4 2020. The mobile attack rate went up to 16.2% from 15% in Q3. This is still a low number considering 35% of all digital transactions are made through the mobile channel. However, there is a significant variance in the mobile attack rate depending on industry, with the media industry having the highest proportion of mobile attacks at 28.5%

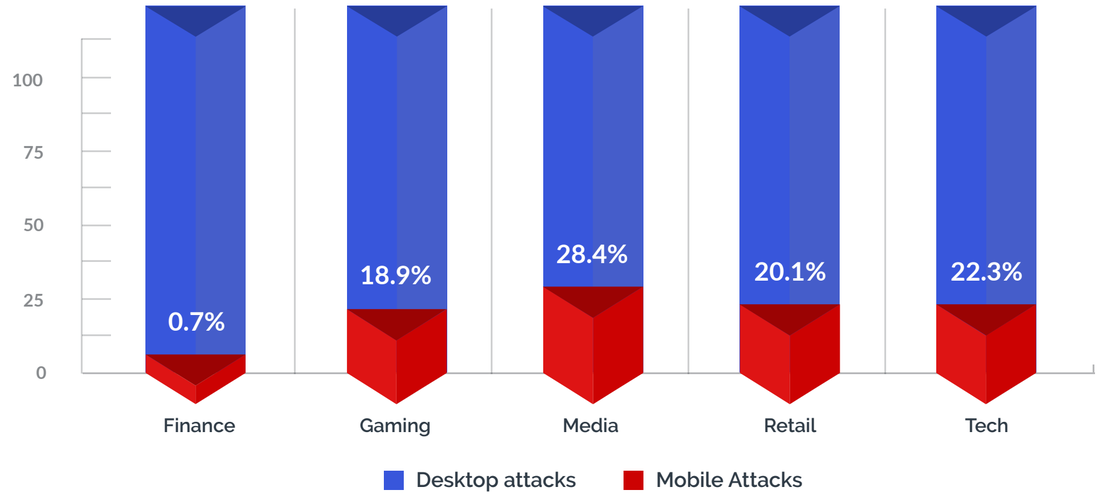
## Q4 Attacks by Device




## Mobile Attack Rate by Use Case



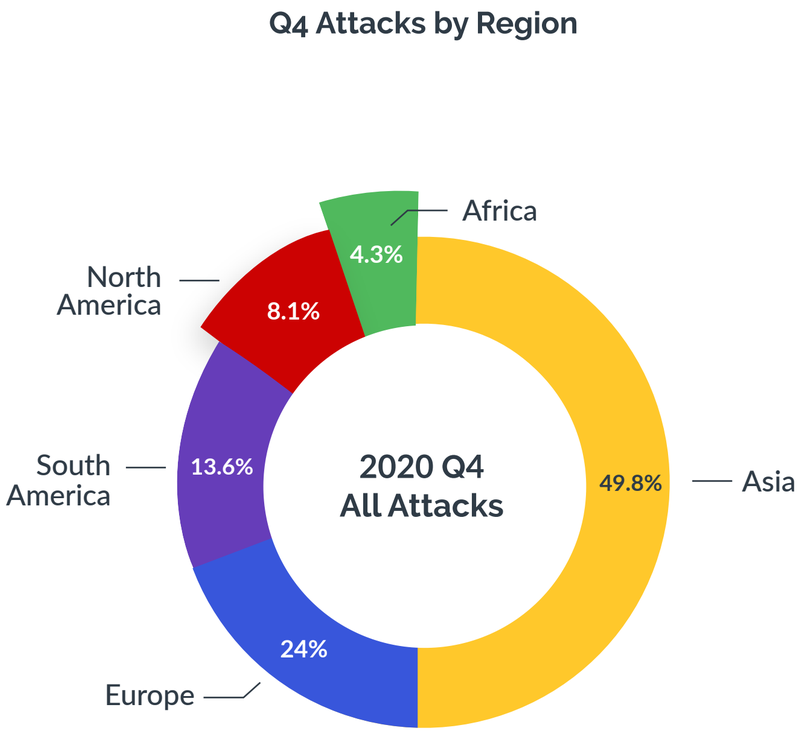

## Mobile Attack Rate by Industry



# Asia Returns to the Forefront of Fraud at the End of 2020

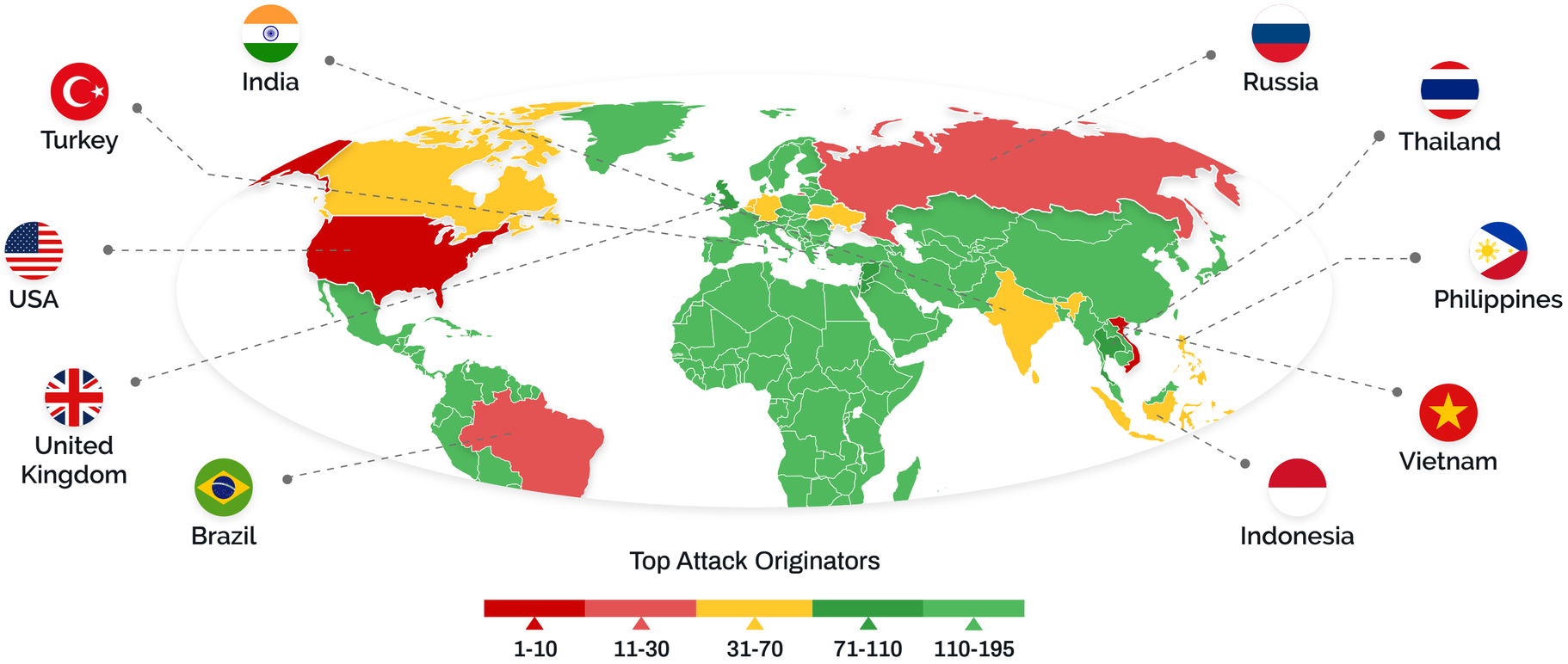
2020 has been a  year where fraud attacks have shifted, with geographies such as the  EU and North America becoming hubs for fraud. However, in Q4 there was a once again in attacks originating from Asia. While the EU and North America are still seeing elevated attack numbers, there was an even more massive uptick in attacks from Asia. This can be partially explained due to fraud attacks around Singles Day -- an even bigger online shopping holiday than Black Friday.

Furthermore, as lockdowns eased and economies recovered somewhat in the western world during the end of the year, less people turned fraud that when the pandemic first hit and millions were unexpectedly plunged into financial distress.

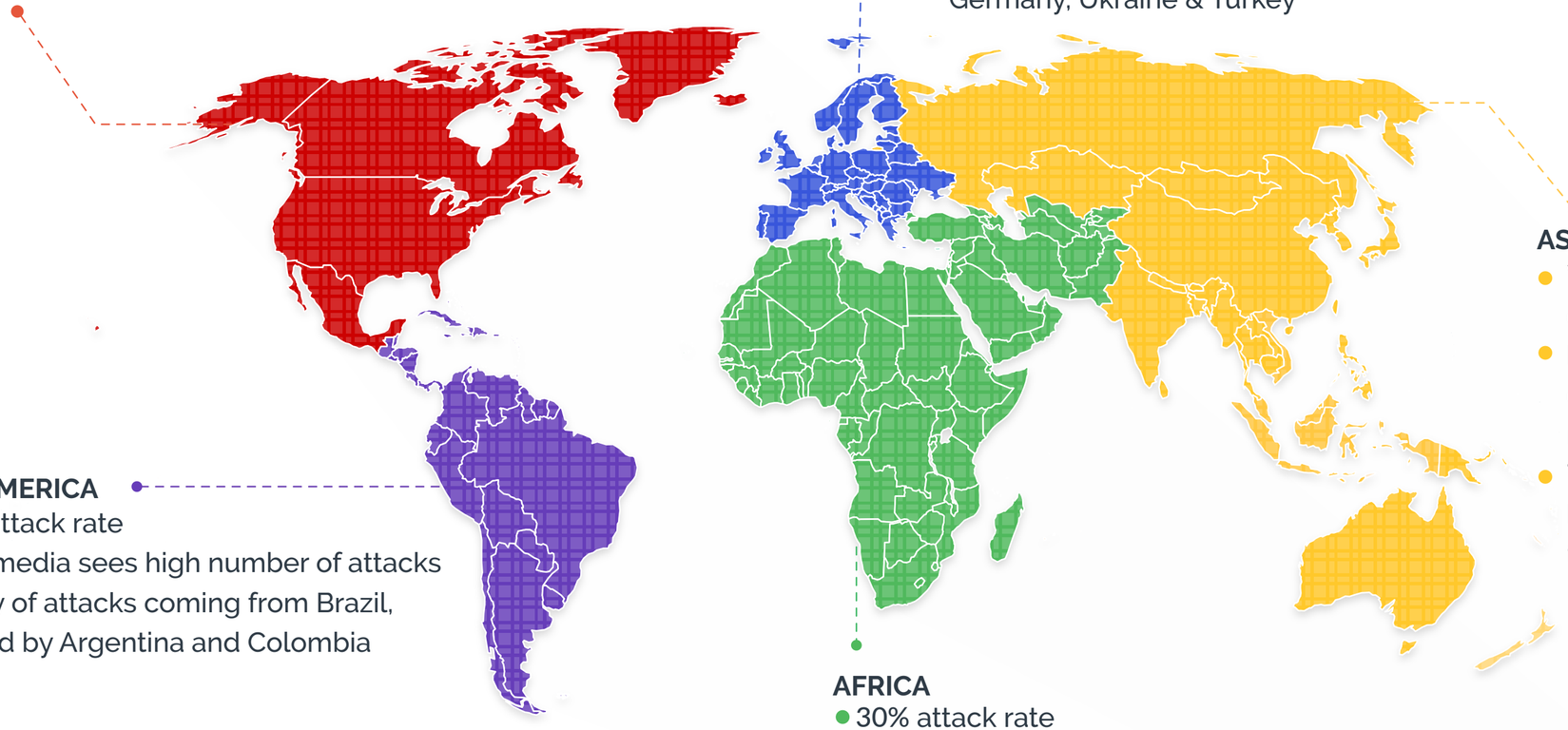


# Top Attacking Countries in Q4 2020

There was a 32% increase in the volume of attacks coming just from the top ten attacking countries in Q4, a list which features nations from all corners of the globe. While the U.S. featured as the top country of origin for fraud attacks in Q4, many of the traditional fraud hubs in Southeast Asia reemerged as top attackers. Vietnam, Indonesia, the Philippines, Thailand and India all appeared in the top ten this quarter. In Europe, Russia dropped from the most attacking nation to the fourth, and there was also a great deal of malicious activity coming from the UK and the Netherlands.



# End of 2020: Regional Attack Trends



### NORTH AMERICA
- 24.2% attack rate driven by bots
- 1 in 5 social media transactions an attack
- 17.5% of retail transactions are an attack

### EUROPE
- 39% attack rate, driven by bots
- Attacks focused on online dating & gaming
- Top attackers: Russia, Netherlands, Germany, Ukraine & Turkey

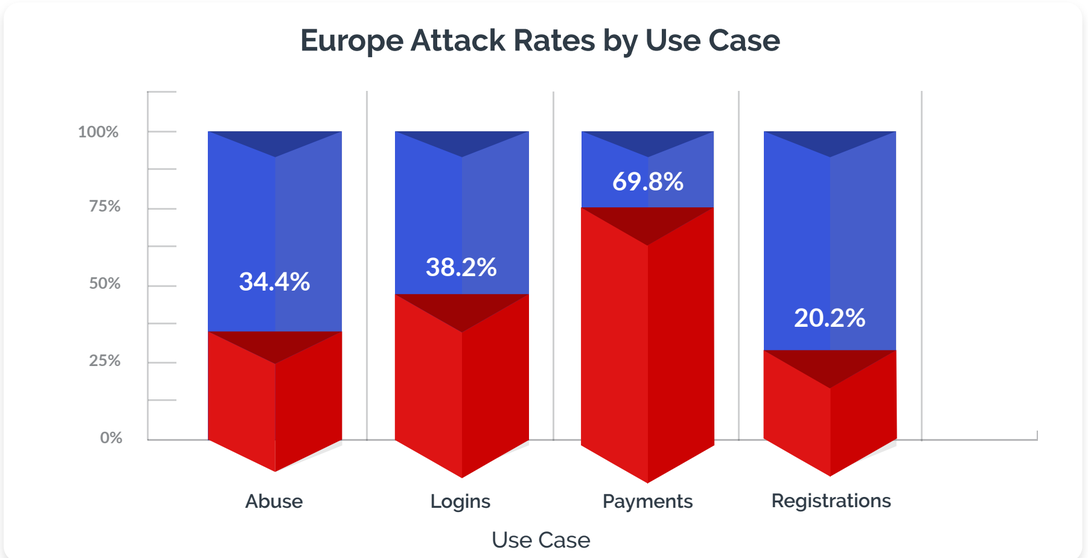
### ASIA PACIFIC
- Very elevated attack rate of 40%
- High attack rates across dating, media, gaming & retail
- Top attackers: Vietnam, India, Indonesia, Thailand & the Philippines

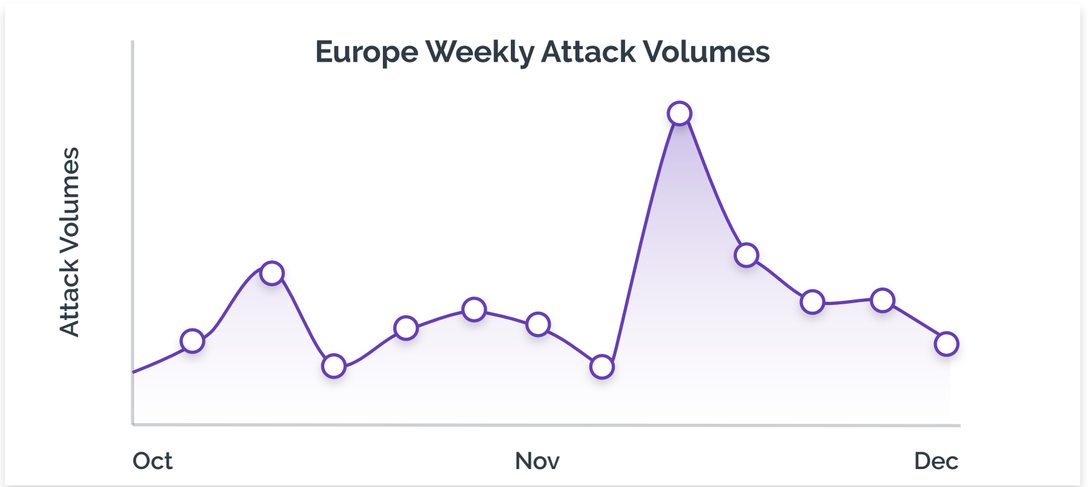
### SOUTH AMERICA
- 30.5% attack rate
- Digital media sees high number of attacks
- Majority of attacks coming from Brazil, followed by Argentina and Colombia

### AFRICA
- 30% attack rate
- Top attacking countries from Northern Africa (Egypt, Morocco, Algeria & Tunisia) and South Africa

# Spotlight on Europe: Key Regional Trends

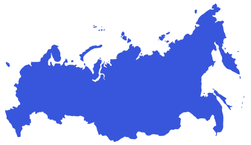
Europe was among the hardest  the hardest hit geographies by COVID-19, and many European countries dealt with  second-wave lockdowns during Q4. That led to record low for sales for physical stores by the end of 2020, driving much of commerce online. The peak in attacks centered around Black Friday, with a particularly high attack rates on payments. This led to a 39% attack rate in Q4 2020, driven largely by bot volume. There was also a great deal of fraud and abuse focused on online dating and gaming companies, as fraudsters sought to scam a largely homebound populace. Europe also saw a high rate of human-driven fraud for fake account registrations at 22.5%.




**39%**
Attack Rate
on European Traffic

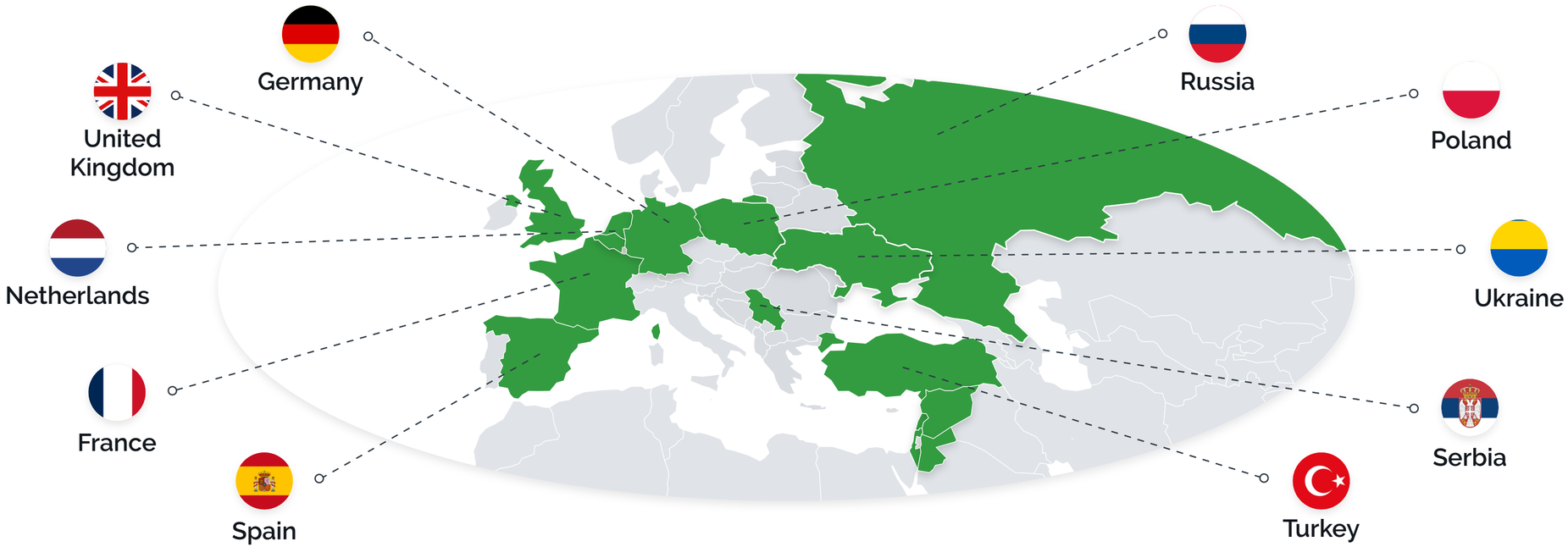
**464M**
Attacks



**Russia**
Top Attacker

# Spotlight on Europe: Top Attacking Nations

Unsurprisingly, Russia was the top attacking country but was joined by non-typical fraud nations the Netherlands, and Germany, as well as Ukraine and Turkey. While attacks are high from certain part of Western Europe in 2020, a massive 52% of all EU-based attacks still originated from Russia in Q4. When it comes to human-driven attacks, Russia also topped the leaderboard, followed by the United Kingdom. This is not typically a hotbed of human fraud, but the country is being hit by repeated lockdowns and economic turmoil due to Covid-19.



# Retail: Spike in Human Driven Fraud

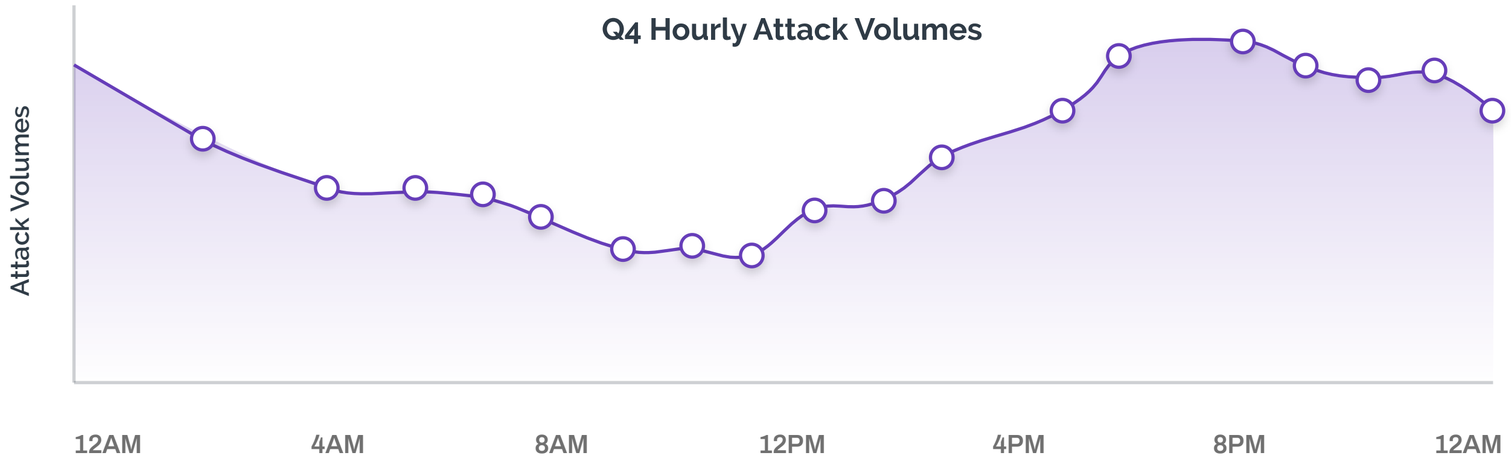
**16%**
Attack Rate

**20%** of Attacks from Sweatshops

**19.5%** of Attacks on Mobile

Retail had the second highest attack rate in Q4 2020, with nearly one fifth of traffic representing an attack. There was an expected spike as consumers and fraudsters alike flocked to ecommerce sites for holiday shopping deals. From Black Friday until the end of the year there was elevated attack levels and sustained fraudulent attempts.

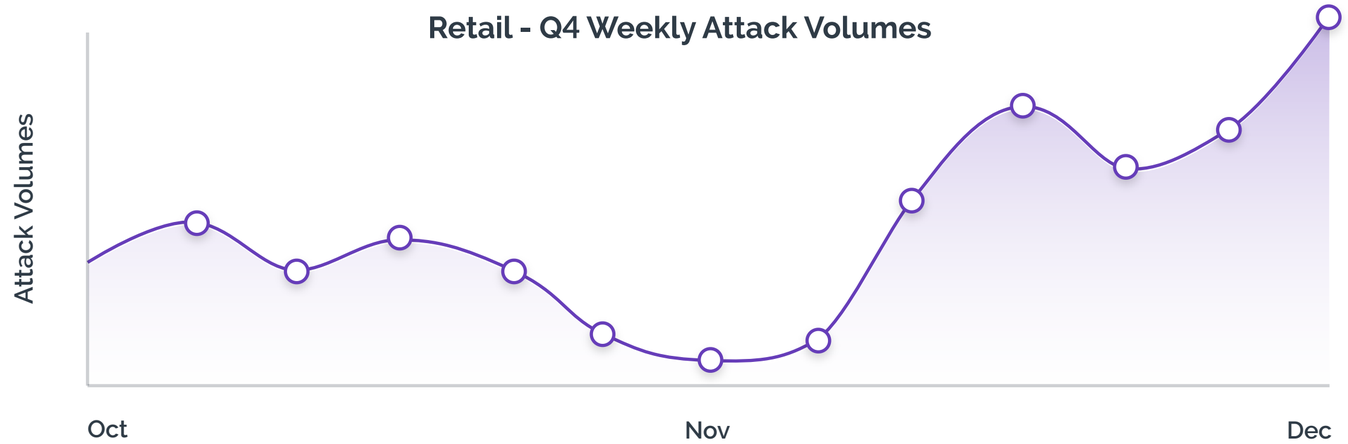
Of note is that 20% of attacks on ecommerce were from human sweatshops, a much higher rate than other industries, and second only to online dating. This demonstrates how hot a target retail sites are at this time of year; attackers are willing to put time and effort into attacking, beyond high velocity bot attacks. We can see the chart of hourly attacks that the volume attacks varies greatly throughout the day. The attack rate is generally quite low during daytime hours, with the increase in attacks in the evening coinciding with elevated good user traffic. However, the high level of attacks that happen during the night and early hours are down to bot activity and cross-border attacks.



# Gift Card Fraud Doubles in Q4

Gift cards became the hot holiday gift this past year, as consumers shied away from physical stores, and many were wary of ordering gifts online due to potential shipping delays. Fraudsters, too, love targeting gift cards as they offer an instant route to monetization and are hard to track, much like cash. It provides quick money and generally an easy getaway.

This year in particular electronic gift card fraud was rampant during the holiday season. There was well over double the volume of fraudulent attempts on gift card transactions in Q3 versus the previous quarter, showing the impact of the holiday shopping season.  Fraudsters use botnets to brute force attacks on gift card websites by testing thousands of card number and PIN combinations per minute. They also use bots and sweatshops to continually check the card balances and redeem them. They hack into a user account and abuse the auto-load feature to drain the account of the funds.




**3.6 Million**
Attacks

**13%**
Attack Rate

**2.4x** attacks
in Q4 vs Q3

# eComm Case Study: 54% Reduction in Fake New Accounts

A global e-commerce company was having an issue stopping fake new account creation. Bad actors would employ bots to create new accounts at scale, which could then be used to commit a wide range of downstream fraud. Its homegrown fraud solution was ineffective at stopping these attacks at scale and also hindered the user experience.

- Fraudulent account registrations
- Bot-driven abuse
- Fake reviews & ratings
- Fraudulent item listings
- Spam messages to good users
- ATO attacks

## Solution

The company deployed Arkose Labs on the new account creation and login flows. The client and Arkose Labs collaborated on tuning the platform to accurately identify attack types,and user behavior. The platform was able to adapt to real-time signals and changing traffic patterns to determine the intent behind traffic to the client's site. Suspicious traffic was triaged into either trusted or potentially fraudulent. Suspicious traffic was served an enforcement challenge; these are designed against the latest innovations in machine vision technology and cannot be solved by bots. Furthermore, Arkose Labs challenges were white-labeled to provide a seamless and on-brand user experience.

## Results

The company immediately saw a 54% reduction in fraudulent new accounts created as compared to the incumbent solution. The company also realized a significant reduction in downstream abuse and chargebacks because of the early detection of fraud attacks by Arkose Labs. In one specific case, the company was able to identify and stop a sweatshop attack originating from Bangladesh that it otherwise would not have detected prior to implementing Arkose Labs.

# Financial Services Application Fraud

**2.6%**
Attack Rate

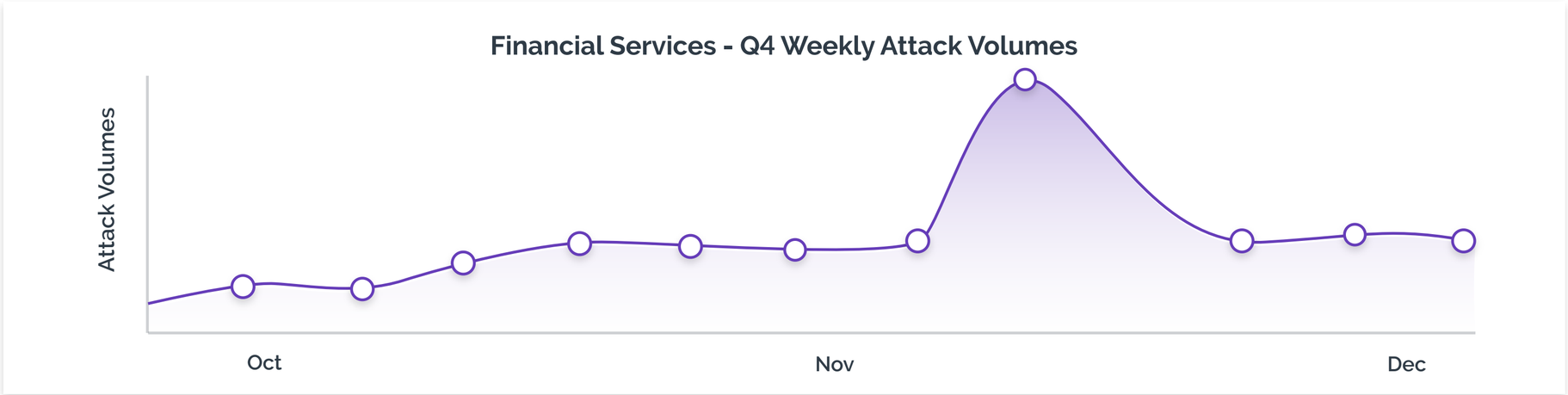
**Registrations**
Top Attacked

**58%** of Transactions on Mobile

Financial Services is an industry that saw an increase in fraud during 2020, they were deluged with fake credit card and personal loan applications, as well as fraudsters targeting government programs meant to help small businesses, such as the PPP.

The first step in being able to carry out these various forms of financial fraud is to open fake accounts using stolen or synthesized identity data. In Q4 the Arkose Labs network saw 720k attacks on financial services companies, with these primarily focused on application fraud. The earlier that businesses can spot malicious account openings, the better they are protected from downstream issues.

Financial services also had the highest percentage of mobile transactions out of all  industries- at 57.8% This continues a years-long trend of consumers ditching physical branches and conducting their financial lives online. Mobile-centric fraud and security should be a top priority for financial institutions.



# Case Study: A Better Digital Banking Experience

Arkose Labs worked with one of the largest global banks, which was facing frequent attacks targeting user accounts. Fraudsters used bots to power credential stuffing attacks at scale, account takeovers, and new loan and credit application fraud. The client had relied on an older, legacy solution for fraud prevention and authentication, but these were ineffective at stopping automated attacks.

**Bot attacks** | **Credential Stuffing** | **Account Takeover** | **Application Fraud**

The bank deployed Arkose Labs to stop the wave of these attacks. Taking a unique approach to fraud prevention and user authentication, the Arkose Labs platform undermines the financial incentive behind fraud, thus dissuading bad actors from even launching attacks in the first place. The Arkose Labs Fraud and Abuse Platform combines real-time intelligence, rich analytics, and adaptive step-up challenges to progressively diminish the profitability of attacks while adapting to evolving attack patterns. Arkose Labs' custom enforcement challenges are context-based, adaptive visual challenges that will thwart large-scale account takeover attempts.

The Arkose Labs Fraud & Abuse platform allowed the bank to drastically slash the number of successful attacks, protect genuine users, and ensure a safe digital banking experience for all customers. Furthermore, a dedicated managed services team works with every Arkose Labs client to ensure the platform is always fine-tuned to deal with the latest evolving threats. Arkose Labs regularly provides custom insights to the bank, allowing it to adapt and alter its own internal fraud controls as needed.

# Media Transactions on Mobile Targeted in Q4

**11%**
Attack Rate

**10.5%** of Attacks from Sweatshops

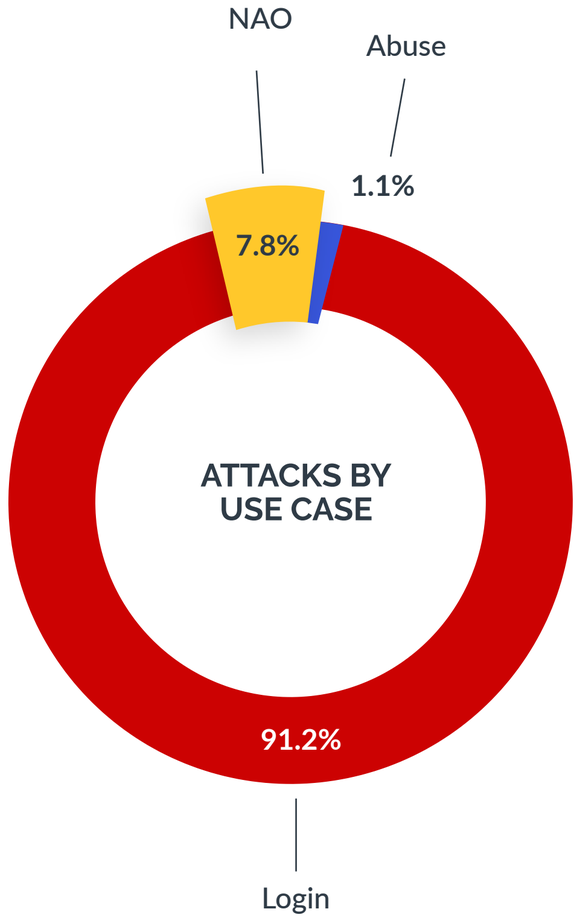
**28.5%** of Attacks on Mobile

Media companies on the Arkose Labs network -- which includes all online streaming and entertainment companies, along with social media and online dating platforms-- had an overall attack rate of 11% during Q4 2020. This was elevated on social media sites, which had an attack rate of 16%.

This vertical had the highest mobile attack rate, with 28.5% of all attacks originating from a mobile device. Overall, 47% of all transactions in these industries occurred on the mobile channel.

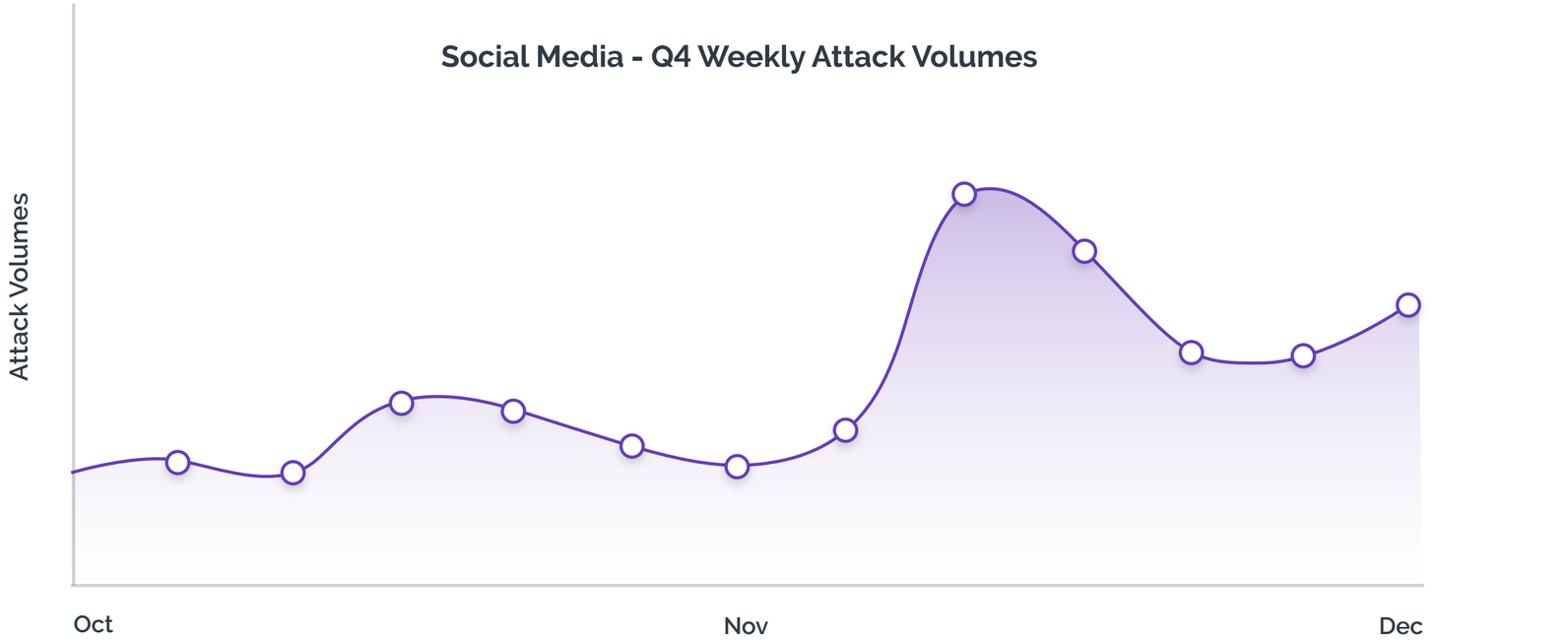
Nearly half of all transactions on media platforms are on mobile, and consequently there is a high mobile attack rate - with 31% of malicious activity on mobiles versus desktop. The mobile attack rate is even higher for human-driven attacks, with 55% of these targeting mobile transactions.

As per the chart, these attacks were mostly focused on the login stage. This is due to fraudsters targeting streaming account credentials to then re-sell on black market sites, and social media accounts targeting for hacking.



# Social Media - High Rate of Mobile Attacks

Being a very mobile-centric industry, it's not surprising that 46% of social media interactions were on the mobile device, with a 28% mobile attack rate. Despite not being a typical retail industry, social media platforms also saw an uptick in attacks on Black Friday and throughout the holiday season. As the practice of spreading disinformation rises, expect social media to continue to be targeted as fraudsters seek to take over legitimate accounts to spread propaganda.




**50 Million**
Attacks

**7 Million**
Human Driven Attacks

**65%**
Attacks on Logins

# Gaming: High Volume Desktop Attacks

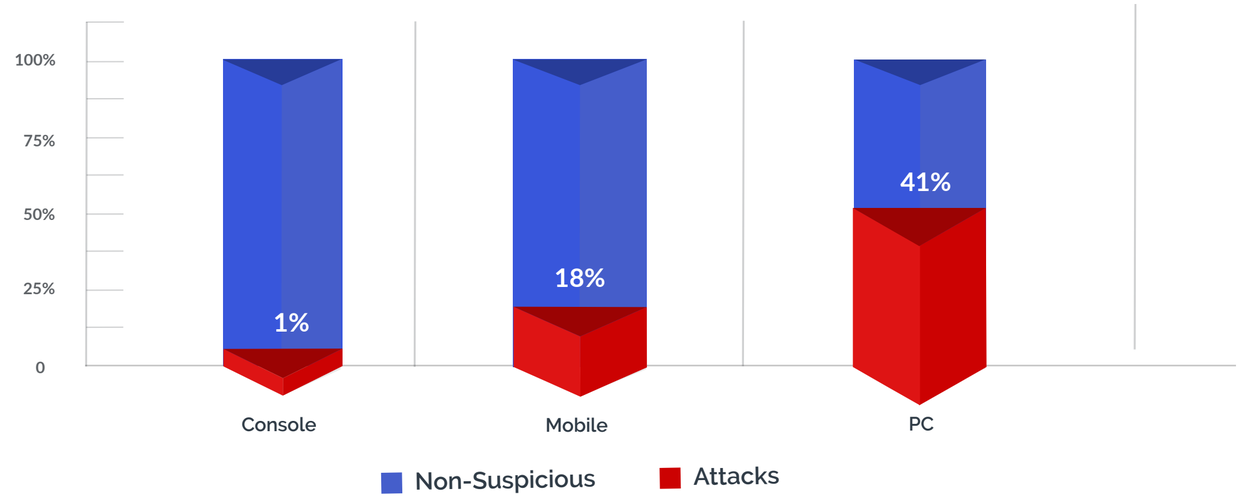
**33%**
Attack Rate

**19%**
Mobile vs Desktop Attack Rate

**99%**
Bot Attacks

Online gaming was the most attacked industry throughout 2020 and that remained the same in Q4 with the highest attack rate, at 32.7% Gaming platforms are barraged with bot attacks, which account for the very elevated attack rate. Attackers launch high-volume campaigns, targeting multiple consumer touchpoints. The massive influx of new users on these platforms amid the pandemic means that incentive levels to attack are sky high. Many online gaming platforms feature intricate digital worlds and virtual economies, which provide numerous unique routes to monetization including farming and reselling in-game gold and real money trading.

Taking over high value gaming accounts is a big target, and attacks on the Arkose Labs network were mostly focused on the login. 35% of all transactions in this sector were on the mobile channel, with a 19% mobile attack rate; attacks rates on gaming consoles were incredibly low.



# Gaming Case Study: Protecting the Virtual Economy

One of the world's most well-known gaming franchises was drawing the attention of bad actors seeking  to exploit its popularity by targeting other players with phishing and scams to obtain user's personal information. They also carried out bot-driven abuse to amass valuable assets within the in-game economy, which can be sold on for real money.

## Solution

After reviewing several possible fraud solutions, the company chose Arkose Labs to stop this bot activity that was ruining the game experience for good users. Arkose Labs was used to detect suspicious behavior and bot activity; the platform analyzes traffic to assign a risk classification, and then uses innovative enforcement challenges to remediate attacks in real time. Challenges use an innovative approach with 3D visuals rendered in real time, which are designed against the latest innovations in machine vision technology. This means that unlike other legacy solutions, even the most sophisticated bots on the marketplace cannot solve them. In this way Arkose Labs helped the company accurately prove which accounts were bot-driven and disrupting the in-game experience for good users. This enabled its internal fraud teams to build a case against suspected bad accounts to ban them and prevent future abuse.

## Results

Very shortly after deploying Arkose Labs, the company was able to slash the amount of successful automated attacks, to protect genuine users and ensure the integrity of activity on its auction house. Just as importantly, real players were not faced with an onerous authentication experience that required them to jump through hoops to prove they are legitimate. This delivered a better customer experience than legacy approaches using challenges with poor good user pass rates or forcing users out of band for MFA,

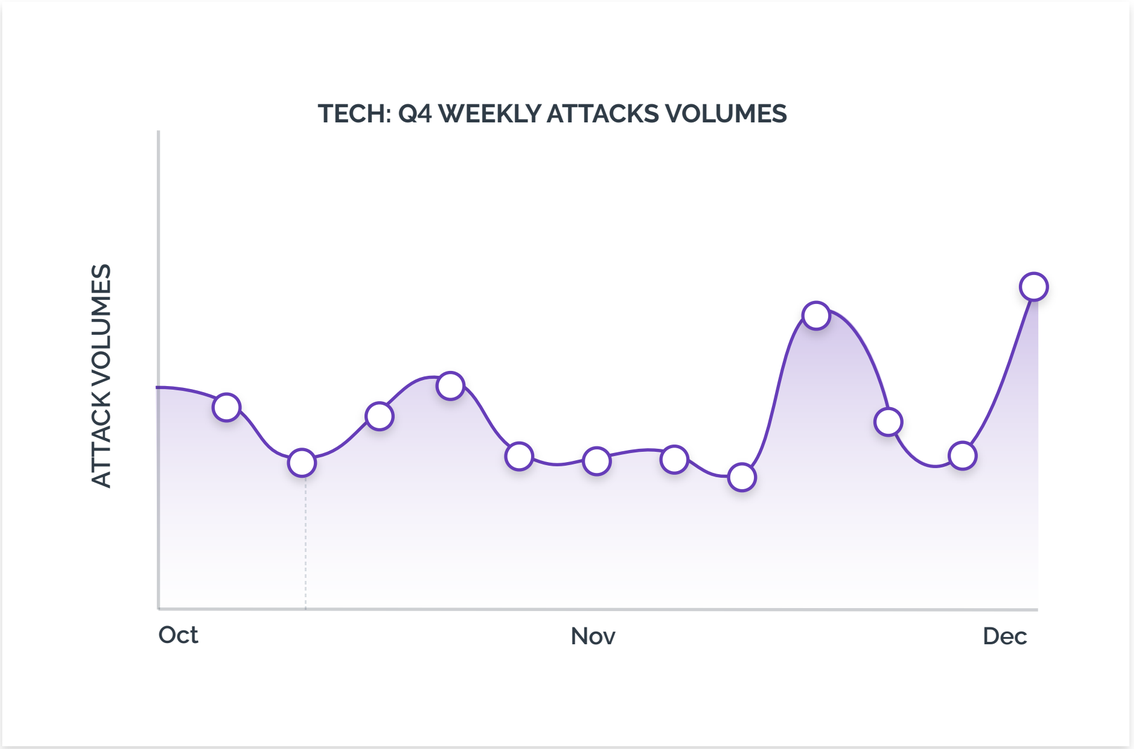
# Tech Platforms Targeted with Bonus Abuse

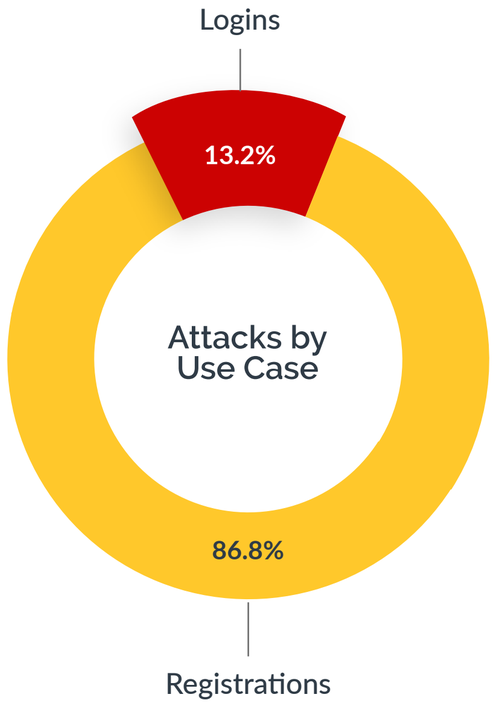
**6.2%**
Attack Rate

**30%** of Attacks from Sweatshops

**22%** of Attacks on Mobile

Cloud-based tech platforms saw a 6.2% attack rate in Q4. Fake new account openings were a major attack vector in this industry, with 22,480,591 such attacks recorded. This is primarily due fraudster's opening new accounts to take advantage of promotional offers at scale. This sector also saw a high sweatshop attack rate, with 30% of attacks being human-driven. Tech saw a 22.2% mobile attack rate, with 28.5% of all transactions overall made through mobile devices.



# Conclusion

Fraud attacks became more frequent and more severe once the world was plunged into lockdowns related to the Covid-19 global pandemic. As we ease back in to something more resembling normal, don't expect fraud to return to previous levels along with it.

In fact, 2020 ended with a massive spike in fraud attacks in all industries from Black Friday onwards, as consumers flocked online in even greater droves than before. If nothing else, fraudsters are opportunists and will continue to quickly jump on any chance to launch a successful attack.

As we move forward into 2021, expect to see the high levels of credential stuffing that occurred in 2020 to continue, as attackers test stolen credentials to repeatedly launch ATO attacks. Account takeovers are so critical to fraud not just because of the valuable personal information that can be used therein, but also for the basis to launch any number of downstream attacks as well.

As more consumers engage in digital commerce, we will see companies offering more and more promotions and bonuses in order to entice customers in this competitive landscape. This in turn will lead fraudsters to open new accounts at scale in order to take advantage of these promotional efforts meant to attract new customers.

Fighting fraud may be more complicated than ever, but with the right approach and the right tools, we can stop the bad guys in their tracks while still maintaining a great digital experience for customers.

# About Arkose Labs

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
arkoselabs.com 

## Offices

**San Francisco**
250 Montgomery St 10th Floor, San

**Brisbane**
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo