Arkose Labs

Ebook

The Long Tail of Covid-19

How the pandemic will continue to shape fraud in 2021

2020: A Year Unlike Any Other

2020 has been a year like no other, as the COVID-19 pandemic has continued to rage across the globe. Fraud thrives in chaos, and 2020 has proven this adage true. Attack volume has gone up significantly compared to 2019, with 2.4 billion attacks detected across the Arkose Labs' network between January and September, compared to 1.3 billion the previous year.

Businesses have been dealing with extremes. With travel and the arts in shutdown and other industries including gaming, social media and ecommerce struggling with unprecedented levels of demand, this year has quickly changed the business landscape. Some retailers broke Black Friday records in April, and others saw an increase in transactions from 100 thousand to 1 million requests per second. This is largely due to the majority of the global population shifting their work and personal lives online as entire countries imposed strict lockdown measures. In a rush to cope with demand and move revenue generating work online, many companies have been playing catch up as they have been forced to continually adapt their operations to deal with the new restrictions and fraud trends.

There has been a spike in human-driven fraud, with fraud farms now accounting for 18% of all attacks. With high levels of unemployment forcing people to seek alternative income streams, the rise of the amateur fraudster has resulted in a significant increase in attacks from mobile devices, which account for 16% of all fraud.

The shift to remote working has seen around 4 billion people working from home worldwide. While this initially caused some problems as companies raced to provide the infrastructure and security measures to support this, there have been unexpected benefits as productivity has been surprisingly high. This is likely to cause lasting changes to work culture as many companies are looking to make this a permanent option.

2020 in Numbers
(Through September)

2.4 Billion
Attacks Detected

16%
Mobile Vs Desktop Attacks

18%
Fraud Farms Vs Automated Attacks

COVID-19 Fraud Trends Survey: Attacks are More Frequent and Intense

The 2020 Fraud Survey polled 80 fraud and security professionals to research fraud trends in the wake of the COVID-19 pandemic. Industry experts came largely from large enterprises from a diverse cross-section of industries, from companies including Netflix, Capital One, Zendesk, Amazon, Wells Fargo, Dropbox, Microsoft, PayPal and Uber. Attack vectors have shifted during the pandemic, and our panelists have reported a growing number of COVID-specific scams.

Credential Stuffing

This is on the rise across all industries, as fraudsters attempt to corrupt the huge wave of new accounts that were created during the crisis.

Social Engineering

People are more isolated than ever, making them easy targets for phishing attacks. New digital users are especially vulnerable as they navigate the internet for the first time.

First Party Fraud

Fraudsters are targeting financial institutions, taking out loans with no intention of repaying them. This has also hampered the processing of legitimate loan applications.

COVID-19 Scams

Official agencies have become a target for impersonation as fraudsters attempt to capitalize on stimulus checks, small business loans and consumer anxiety.

Identity Theft

Children and young people have become increasingly easy targets as they spend huge amounts of unsupervised time logged onto digital classrooms, social media platforms and gaming networks.

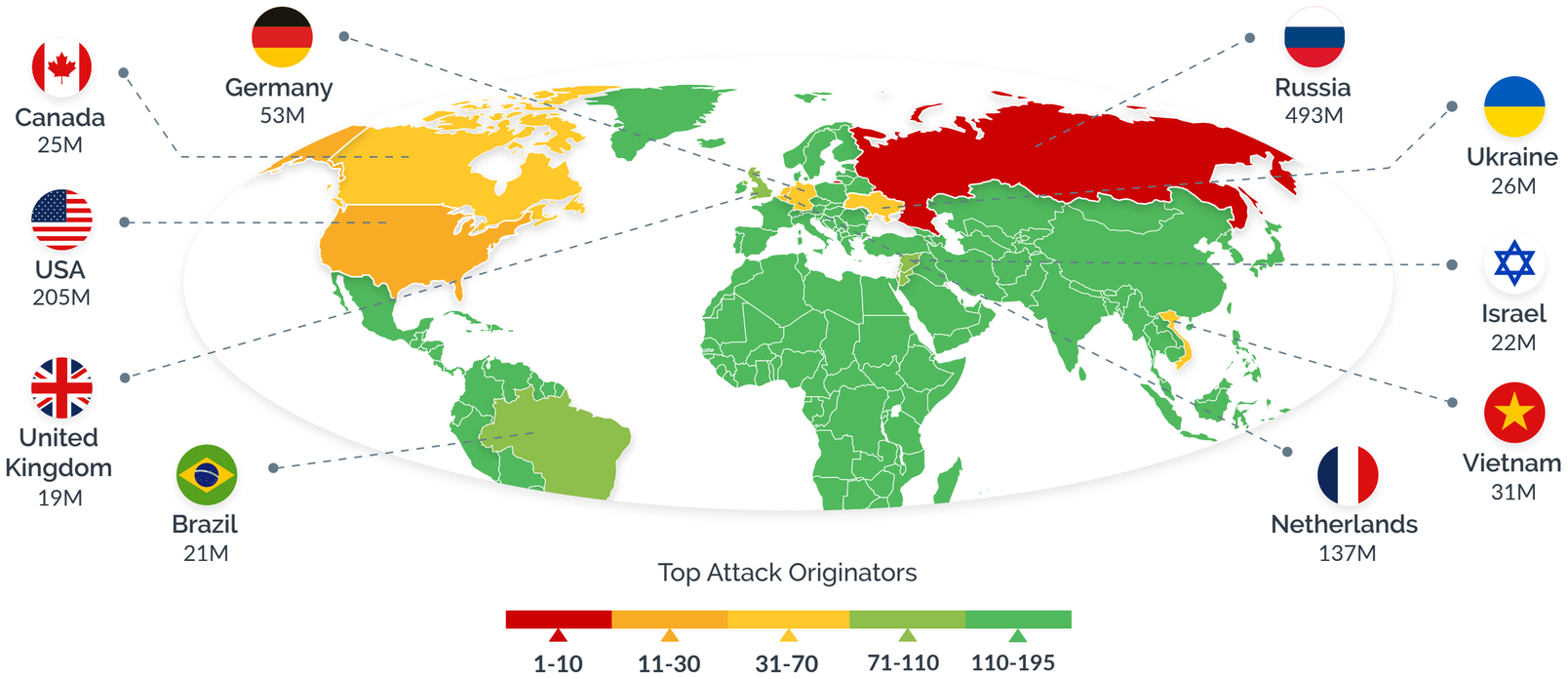
Friendly Fraud

There are increasing reports of chargebacks and friendly fraud as many people face financial hardship and moral lines become blurred.

Top Attacking Countries - Cybercrime in the New Normal

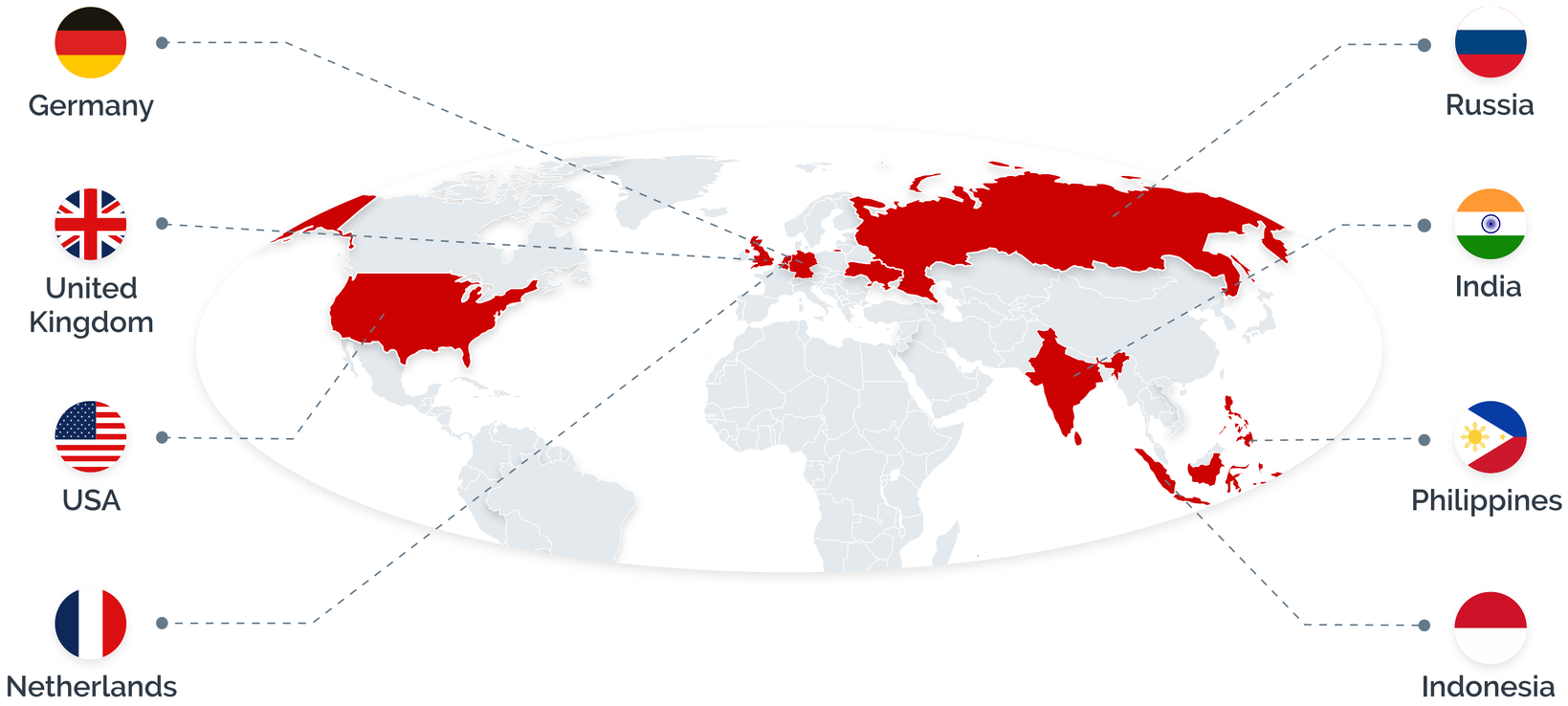
2020 has seen a seismic shift in fraud geography, with attacks increasingly coming from developed economies. Traditionally, fraud hubs have originated in the developing world, with the Philippines topping the charts this time last year. It doesn't even feature in Q3 2020, with the USA, Netherlands and Denmark representing the highest attack volume.

This is largely due to financial hardship. With ever-increasing levels of unemployment as entire sectors operate at minimal capacity, people are seeking new income streams and are crossing previously red lines to make ends meet. This is compounded by a highly efficient and interconnected global fraud ecosystem. Fraudsters are highly adaptable and can quickly pivot their operations to take advantage of changing economic circumstances. They have capitalized on the COVID-19 crisis by recruiting new workers and scaling up attacks.



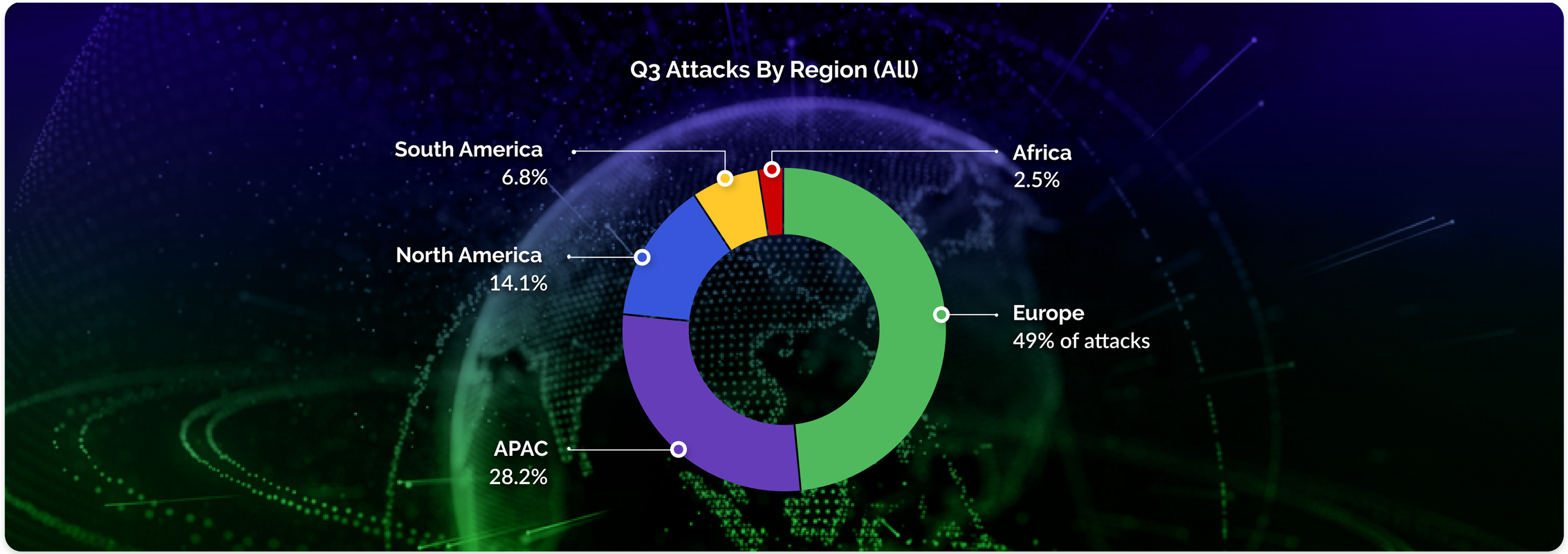
Fraud Farms: Top 10 Attacking Countries

Organized fraud farms of low-skilled, low-paid workers make up a vital component in the fraud ecosystem. They help mount attacks at scale, bypassing fraud prevention systems designed to prevent bot attacks. Due to the higher cost of human-driven attacks, they have traditionally originated in countries with low wages. This year has seen a surprising upturn in fraud farm activity from developed economies including the U.S, Great Britain and the Netherlands, alongside traditional fraud farms hubs such as the Philippines and Thailand.



Regional Trends: Surge in Attacks From Europe

Almost half of all attacks in Q3 2020 came from Europe. This can be linked to the drastic cuts in GDP for many European countries since the start of the pandemic with the UK, France, Italy and Germany all suffering a reduction of 10% or more. Fraud is a business, with profit the main incentive. The spike in attacks from nations seeing the biggest economic downturn highlights the financial drivers of fraud. A massive 64% of human-driven attacks originated from Europe in Q3, with 10 million attacks from Russia and 7 million attacks from the UK.



Friend or Foe? Spotlight on Friendly Fraud

The shutdowns and growing financial hardship caused by COVID-19 have created a surge of friendly fraud. The travel industry is the worst hit, with many businesses seeing a 200-400% spike in chargebacks as holidays were cancelled, and hotels closed for business.

The massive spike in digital traffic has also brought a significant rise in chargebacks to retailers. This is partly due to the economic downturn, but it is more complicated; with physical stores closing their doors, many people started shopping online for the first time. These digital debutants are unfamiliar with digital transactions, and confused by cancellation or refund policies. Supply chain issues compounded this, causing shipping delays that resulted in a rise in illegitimate chargebacks from consumers confused by the system. Some companies simply chose to accept higher levels of fraud in order to let more real customers in, but this is not a long-term solution.

This poses significant challenges for fraud teams: these transactions are often not malicious, and appear to be legitimate because they come from genuine customers. Businesses need to protect their revenue without blocking potentially genuine customers long term. It is crucial that businesses improve communication with customers, and clarify their refund policies alongside taking a tough stance on friendly fraud.

Revisiting Top-Targeted Industries from Q2

Gaming

Gaming platforms have seen major increases in traffic during the pandemic, and as a result, fraudsters continue to ramp up attacks. The industry had a 39% attack rate in the third quarter, which is a major increase on the previous period. 95% of attacks were bot-driven, and 65% came on logins, focusing on account takeover.

Tech Platforms

Despite the massive uptick in traffic as the majority of the global population work from home, there has been a fall in attacks on tech platforms, with an attack rate of only 8%. Interestingly, the attack rate spiked in the second half of August. This is likely to be due to fraudsters targeting virtual education platforms as schools reopened. At least 60 school districts were hit with ransomware attacks.

Media

Social media and streaming platforms were targeted with a wide range of fraud and abuse, with a sharp rise in automated scraping, account takeover attacks and fake account registrations. There has been a growth in attacks from mobiles, which now account for 37% of all attacks.

All About The Money

The economic uncertainty caused by the COVID-19 pandemic has created a fertile ground for fraud. Financial services are seeing a significant rise in attacks, with 70% of attacks at the payment stage. Some of these come from consumers suffering pandemic-related financial hardships who misrepresent their income in a desperate bid to access credit. For the professional fraudster, the sharp spike in digital payments during the pandemic has become a top-attacked touchpoint. This poses a challenge for financial services: consumers expect an instant, frictionless experience, while fraudsters attempt to hijack digital payments undetected.

COVID Finance Trends:

- Fraudsters targeting the influx of stimulus checks and loan applications
- 30% spike in new accounts in the digital investing industry
- Exponential rise in SMB lending from 3,000 apps per month to 100,000
- Credit card companies need to shift parameters as approval rates very low.
- Increase in voluntary money mules, and ATO of children's accounts to launder money.

Pandemic Pitfalls: Challenges For Businesses

A key challenge for businesses in 2020 has been the unpredictability of humans. Traditional fraud prevention strategies are designed to recognize what looks like typical good and bad behavior. This year has been chaotic and thus typical online behavior and traffic patterns were thrown out the window. This is exacerbated as people moved in with parents and worked from home, causing IP anomalies and confusing fraud systems.

Split Personalities

As the economic crisis deepens, more people are turning to fraud. Fraud prevention teams struggle to deal with 'split personality' customers who are genuine customers on one site, but commit fraud on another. This unpredictability makes it difficult for some fraud prevention systems to distinguish between good and bad actors.

Identity Crisis

As real-life shops, workplaces and restaurants closed their doors, people moved their lives online. Face-to-face interactions became digital, warping our concept of identity. Rather than physical identification documents or human characteristics, online identity relies on data. Fraudsters capitalize on this, with easy access to millions of stolen identities and toolkits that enable them to mask their true identity and intent.

Trust Issues

People are experiencing heightened anxiety and distrust as a result of the pandemic. COVID-19 conspiracy theories have been rife, and social media platforms have been hotbeds of misinformation and scaremongering.

Protecting the Most Vulnerable

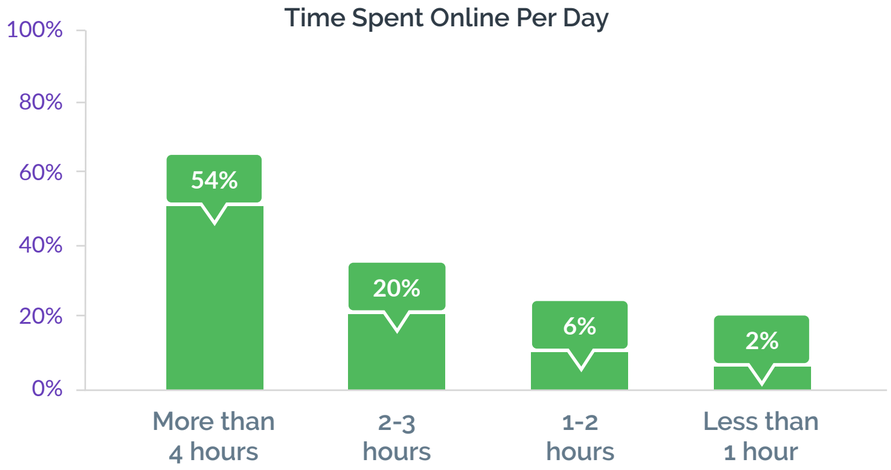
7 months of lockdown life has left young people spending more time than ever online, attending school, gaming, socializing and increasingly, shopping. Arkose Labs commissioned a study of over 80 young people aged 6-16 across 3 continents, and found that 54% spend more than four hours online every day.

Much of this time is spent unsupervised, and while this generation of young people are digital natives, they are extremely vulnerable to scams and other fraud. Young people are falling victim to bullying, sexual abuse, exposure to inappropriate content, social engineering, ransomware, malicious links, and addiction. This abuse can have a lasting impact on children's mental health and serious consequences for their futures.

Schools were forced to move education online very quickly in March, and there were some major security issues with some email accounts set up to use the same username and password. This made it very easy for young people to hack into classmates' accounts and pose as each other. The young fraudster is also a fast emerging trend, with a rise in gaming scams from young people looking to steal in-game currency and bonuses. Online education also opened up new attack vectors, with fraudsters infecting free eBooks with malware.

95%

of children spend more time online due to COVID-19



Protecting the Digital Debutants

Digital security products are rarely designed to be accessible for young people or seniors. There is a huge opportunity for businesses to adjust their services to be inclusive to a wide range of vulnerable users. Indeed, Covid-19 lockdowns have rewritten the target profiles for many companies, as many more diverse people now access these services. This can be a challenge for fraud and security teams in ensuring their profiling of a good user is not outdated. According to a parent survey by SuperAwesome, 96% of parents and caregivers want more control in games and services for young people. It is imperative that businesses step up in the fight to protect young people from cybercrime: ultimately creating safer platforms will lead to customer loyalty and improve the bottom line for businesses.

Many businesses are effectively deploying social media teams to educate customers on fraud, flagging scams and advising on the dangers of sharing personal information. Education is the key to helping these digital debutants safely navigate the digital realm. Companies should be proactive in letting customers know about common pitfalls and how to avoid them.

Another rising consumer base is the over 65s. This group is considered high-risk for COVID-19, and many have been shielding since March, forcing them to adapt to the digital world, sometimes for the first time. They are especially vulnerable to scams and until now, businesses have not focused on building products that protect this group.

Pandemic Positives: A Look on the Bright Side

Despite the hardships of 2020, there have been some silver linings. The extreme spikes and falls in traffic for businesses during lockdown have forced companies to be adaptable and fast-moving. In some cases, demand quintupled, requiring fast engineering solutions to survive. While attack volumes have reached a new high, many fraud teams have successfully stress tested their systems, rooting out weak spots and strengthening their defenses for the future. As a result, they will be more resilient than ever in the face of the next 'black swan' event.

In a year of financial hardships and reduced spending, businesses have become increasingly creative with their approach to customer retention, offering flexible subscriptions and loyalty bonuses. Innovative thinking will stand companies in good stead for an uncertain future.

A major positive is that though the world has been in shutdown, communication across sectors is at an all time high. Competitors are becoming allies as they share information on trends and stand together in the fight against fraud.

With many people working from home worldwide, businesses are seeing high levels of productivity that are likely to make this a long term option for workers. This has led to improved work-life balance, with travel time removed and workers developing strategies to create boundaries between work and leisure time. Businesses are also reporting an improvement in camaraderie in their teams, with many instigating regular check-ins to monitor morale and mental health. Remote working has also had a positive effect on diversity and inclusion in recruitment: without geography as the primary driver for hiring, companies have a much wider pool of excellent candidates. These benefits are likely to become long term fixtures of business culture.

COVID-19: A Look Ahead

Arkose Labs asked a panel of fraud and security experts across multiple sectors for their predictions for the coming months. Here are some of the top responses as to how trends that began during the pandemic in 2020 will continue or evolve into 2021.

Businesses will shift to remote-working long term, leading to the closure of offices in major cities, and a realignment of offices that do stay open.

Supply chain issues causing the delay of goods ordered online will lead to more chargebacks, as consumers become frustrated with lengthy delivery times.

Online traffic will remain at holiday levels on a day-to-day basis,as much of the world shifts permanently online.

Use of digital financial services has rocketed since March, and experts are predicting a permanent cashless future.

In the drive to bring consumers back to physical stores post lockdown, an increase in rewards programmes will also attract high levels of fraud and friendly fraud.

Businesses that have boomed since March will have to focus on long-term sustainability and ensure that they are not just seen as ‘COVID-19’ products.

Advice For Businesses

Streamline Operations

During this time of international crisis, simplicity can be a key to success. Communication is more complicated in a remote work environment, and informal 'water cooler' chats no longer an option. A simple, direct approach ensures efficiency and

Treat Fraud As A Business

Ultimately fraud is just another business, with profit the primary driver. Taking a zero tolerance attitude, and using an approach that saps fraudsters time and resources will slash the ROI of attacks and force fraudsters to take their 'business' elsewhere.

Identity Matters

With increasingly compromised digital identity, businesses will benefit from fraud prevention solutions that assess a wide range of device information and interaction to eliminate identity cloaking tools. Comprehensive risk profiling reduces the risk of false positives and informs secondary screening.

Be Proactive, Not Reactive

Traditionally businesses have accepted some levels of fraud as a 'cost of doing business' which has allowed fraudsters to develop increasingly sophisticated attack patterns over years of attempts. As COVID-19 continues to cause havoc across the globe, serious investment in robust fraud prevention will safeguard profit and reputation.

Prioritize Protecting The Vulnerable

Young people now make up a much higher proportion of internet users as a result of the pandemic. Two-thirds of all US children aged between 9 and 12 are now playing Roblox*. Young people and their parents represent an increasingly powerful consumer group, and safeguarding the vulnerable is both a moral imperative, and smart business move.

Conclusion: Is this the New Normal ?

One phrase that has been ubiquitous since the start of this pandemic has been “the new normal.” And while some aspects of life have regained a sense of normalcy, one thing that will likely remain from the lockdowns is permanently higher digital traffic levels.

With more people than ever online, fraud will remain at historically high levels in 2021 and beyond. Fraud attacks have not only become more frequent, but also more severe. The entry point to commit fraud also continues to become lower; automated scripts are cheap and easy to deploy, and fraudsters can hire human fraud farms to carry out attacks for a minimal investment.

With fraud attacks evolving by the day, businesses must also rethink and reimagine how they fight fraud. Old models of what "suspicious" behavior constitutes are far less relevant. Endpoint solutions to protect against bots that were robust even a few years ago are obsolete today, due to rapid advancements in machine vision technology. Years of massive data breaches have corrupted digital identities to the point where they are meaningless.

That’s why merely “mitigating” fraud is no longer effective. To truly stop it, you must eliminate the financial incentives to commit the attacks in the first place. Only then will we create a digital world that is safe for all.

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

Offices

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

Brisbane
315 Brunswick St, Brisbane, Queensland AU

Schedule Demo