Arkose Labs

2020
FRAUD TRENDS SURVEY

Insights from Fraud and Information Security Professionals on the New Threat Landscape

INTRODUCTION

2020 has been a year like no other, as COVID-19 has wreaked havoc across the globe. Businesses have seen disruption on an unprecedented scale with mass lockdowns worldwide, and millions of people working from home.

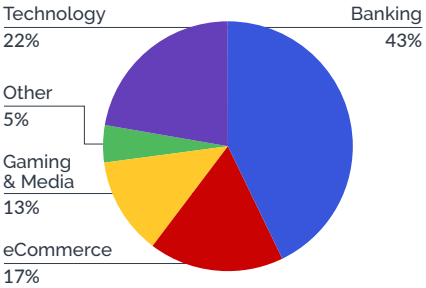
While some sectors such as travel and entertainment have had major slumps in demand, others are thriving due to spikes in online traffic as consumers shift their shopping, socializing and entertainment online. Gaming and ecommerce have seen a massive uptick in activity in 2020. Some retailers broke Black Friday records in April, and transactions increased from 100 thousand to 1 million requests per second for some organizations.

Where traffic increases, so does the profit potential for fraud. Fraudsters are highly adaptable, often pivoting their attacks quickly to reflect shifts in consumer behavior and anti-fraud technology to maximize their ROI. That's a big reason why attacks on the Arkose Labs network doubled in the first half of 2020, versus the second half of 2019. Gaming has been a top target for fraud, with one in four transactions now representing an attack.

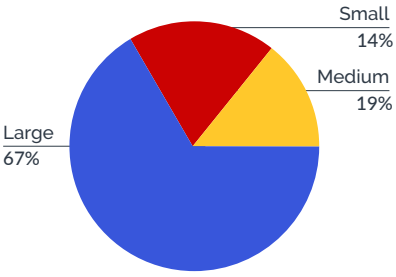
SURVEY PARTICIPANTS

Arkose Labs assembled 80 fraud and security professionals to get insights into 2020 fraud patterns in the wake of the COVID-19 pandemic. Industry experts came largely from large enterprises, from companies including Netflix, Capital One, Zendesk, Amazon, Wells Fargo, Dropbox, Microsoft, PayPal and Uber.

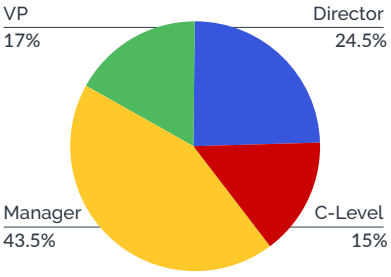
Industry



Business Size



Job Function

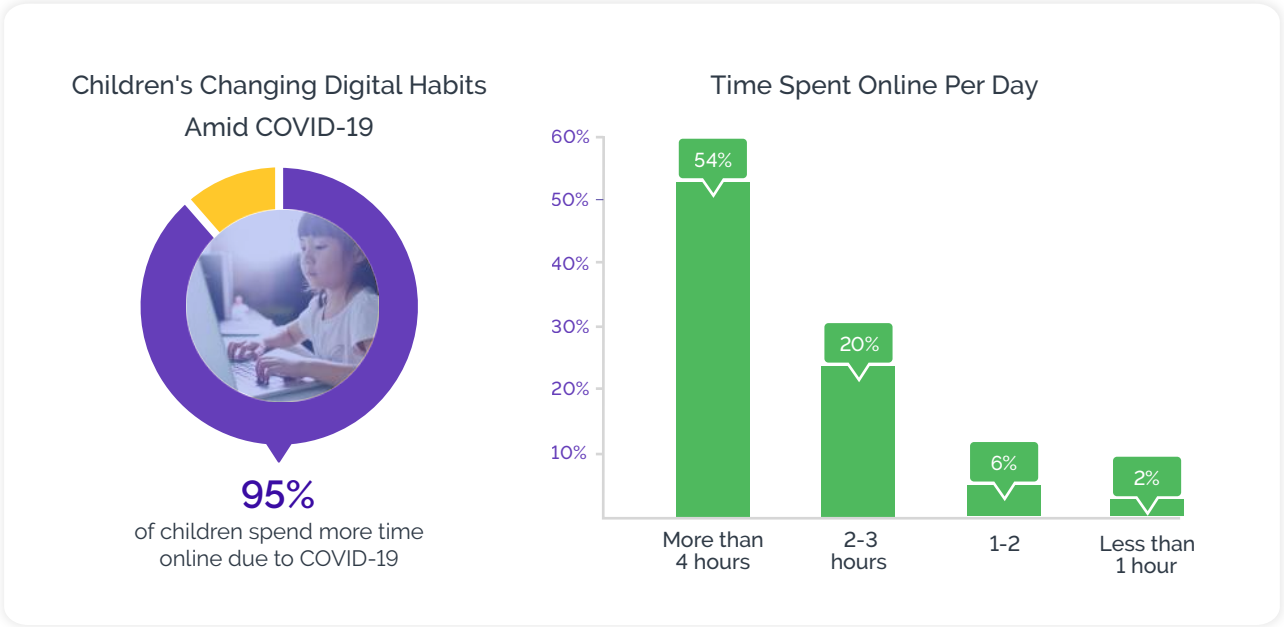


2020: A FERTILE GROUND FOR FRAUD

Fraud thrives in chaos, and 2020 has been a time of unprecedented turmoil in the digital economy. Businesses have had to shift revenue-generating activity online, and while some are booming, others have struggled to get the infrastructure in place quickly enough to protect against fraud. This is compounded by rapidly changing consumer traffic patterns that make it harder to differentiate between good and bad actors using baselines of "normal" behavior.

The economic uncertainty and anxiety around COVID-19 makes fraud incentive levels higher than before. Tens of millions of people have been cast into unemployment, and are now seeking alternative sources of income. Fraudsters have been quick to exploit this, luring previously legitimate workers into cybercrime, dramatically increasing their potential workforce.

Furthermore, there has been a huge increase in potential victims as even the staunchest technophobes have been forced to move their lives online. This has widened the internet user demographic with both the young and elderly interacting digitally, sometimes for the first time. These digital debutants are particularly vulnerable to fraud and there has been a slew of scams and fraud attacks targeting these groups.



KEY TRENDS: REPORTS FROM THE FRONTLINE

Credential Stuffing

Experts across all sectors are reporting an increase in credential stuffing attack volume as fraudsters try and launch automated attacks at scale. However, they are also seeing fraudsters getting sloppier, for example, using invalid browsers. Effective protection against automated attacks is resulting in stable fraud losses from this attack vector for many organizations.

Account Takeover

Targeted ATO attacks are also on the rise, with some businesses experiencing levels usually only seen at Black Friday and holiday shopping peaks. Organized human-driven attacks have increased, as well as hybrid attacks that blend automated and human resources to carry out highly orchestrated, multi-step attacks.

Social Engineering

An increased portion of the global population is living and working in semi-isolation, disconnecting them from their peers and normal points of reference. With less collaboration and oversight, people are more vulnerable to malicious content, phishing scams and identity theft. This is especially true for digital debutants, who are specifically targeted with social engineering scams.

Friendly Fraud

There has been a significant rise in chargebacks and other forms of friendly fraud. The financial hardships caused by COVID-19 have blurred the lines of what is acceptable, and previously good actors are also engaging in promo and bonus abuse.

Identity Theft

Children have become a new target for identity theft, as they have spent most of the year logged onto digital classrooms, social media, and gaming networks. They are often unsupervised and are seen as easy prey by fraudsters.

COVID Scams

There is a wide range of COVID-specific scams that exploit consumer anxiety around the pandemic. Government and health organizations are prime targets for impersonation due to their perceived authority. There has also been a notable rise in fake charities.

Griefing

Unlike most fraud, profit is not the motivator here: gaming platforms are seeing the results of trolls in lockdown, with an explosion in griefing, the act of intentionally harassing or irritating other players.

First Party Fraud

Financial institutions are witnessing highly elevated levels of first party fraud, where individuals take out lines of credit with no intention of ever repaying it.

COVID-19: CHALLENGES AND SILVER LININGS

For large parts of 2020, real life interactions became entirely digital. This has further warped our perception of identity: online identity is based on data rather than human characteristics or physical identification documents. This is easily manipulated by fraudsters, who have access to millions of stolen credentials and toolkits that allow them to disguise both identity and intent.

This is further complicated as more people turn to fraud, blurring the line between good and bad actors. Respondents described the problem of dealing with 'split personality' customers who can be both a genuine customer on one site, and a fraudster on another. The erratic shifts in consumer behavior make it very difficult for some fraud prevention solutions to identify 'normal' behavior patterns.

The huge spikes in traffic across ecommerce, gaming and social media platforms during lockdown required businesses to be adaptable and fast-moving. In some cases, infrastructure loads quintupled and required fast engineering solutions to keep up with the demand. The crisis also called for a creative approach to customer retention as people tightened their belts and cut their spending. A flexible approach offering users the option to pause their subscriptions has proved successful in many cases.

Fraud prevention teams are also battling against increased anxiety and distrust. Social media platforms have been key targets for misinformation campaigns, and in a USA election year this is particularly insidious. COVID-19 related conspiracy theories have abounded, and this is making it increasingly difficult for people to distinguish between real and fake news.

A huge positive coming out of the pandemic is a more collaborative approach to fighting fraud. Competitors have become allies as companies share information on fraud trends and are presenting a united front against fraud.

For some businesses, COVID-19 has increased traffic and attack volume to unprecedented levels. This has enabled fraud teams to stress test their systems, identifying weak spots and strengthening strategies for the future.

THE IMPACT OF REMOTE WORKING

The effects of working from home are likely to be long lasting, with fraud departments across many sectors and geographies shifting to this model. Offices are being closed in big cities, and there is extensive discussion around relocation to smaller, less expensive sites. This presents some positives with many workers enjoying a better work-life balance, but also raises uncertainties over the future of some jobs.

While there are some benefits, with many organizations reporting increases in productivity, fraud and security executives are reporting certain challenges. Information can be easily siloed between teams, with no chance of conversations happening at the watercooler.

Communication is more contrived, with every conversation needing to be scheduled, which can affect cross-functional collaboration. Respondents stressed the importance of continued interaction between front end app makers and fraud prevention teams. Workers in all areas are having to be adaptable and creative in their approach to problem-solving.

A FOCUS ON FINANCE & PAYMENTS

Fintechs and banks are seeing an uptick in consumer fraud as unemployment and poverty levels rise. In a bid to access credit, people are increasingly misrepresenting their income, which will have a lasting effect on loans.

The COVID-19 pandemic is set to be the final nudge for societies to fully embrace digital payments. The use of cash is decreasing as consumers and businesses prioritize hygiene and avoid human contact. While some ATM networks are reporting that cash withdrawals have rebounded, the industry is facing some big existential questions, such as whether we are moving to an entirely cash-free economy.

Customers expect a frictionless experience alongside robust security. This poses challenges for fintechs and banks, who are also navigating a highly complex regulatory landscape. Fraudsters are not bound by regulation and use this advantage to hijack payments before any party is aware.

TAKEAWAYS: ADVICE FROM THE EXPERTS

Respondents warned against becoming too comfortable: there has long been an attitude that considers some fraud as part of the 'cost of doing business'. This has allowed fraudsters to hone their tactics as they develop ever more sophisticated attacks over years of attempts. Fraud is a thriving business and profit is the primary aim. It is more crucial than ever to take a zero tolerance approach, that slashes the ROI of attacks, forcing fraudsters to go elsewhere.

There is recognition across all sectors that during a time of international crisis, simplicity can be key. Communication is more complicated in a remote work environment, and a pared down direct approach maximizes efficiency and reduces confusion.

In a world where digital identity has been compromised, identity management needs to be viewed as an entire lifecycle rather than just done at the point of registration. Businesses are benefiting from intelligent fraud prevention solutions that assess a range of device information and user interactions to root out automated attacks and fraud "sweatshop" activity. Detailed risk profiling provides a powerful basis for secondary screening, and reduces the danger of false positives. This approach safeguards customer security and ensures a smooth user experience.

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

Mail:

support@arkoselabs.com

Address:

USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006

Schedule Demo