Arkose Labs

# COVID-19 & Fraud: A Black Swan Event

## The Unexpected Opportunity for Fraudsters

# COVID-19: The Black Swan Event

A black swan event describes a catastrophic event that is so rare and unexpected that even the possibility that it might occur is unknown. The COVID-19 crisis is such an event, bringing overnight changes to the way we interact and transact.

While some sectors have ground to a halt, or are scrambling to move revenue-generating activity online, others are grappling with an overnight explosion in demand. Large numbers of the world's population are adjusting to working from home and carrying out more of their daily activities virtually - all amid an atmosphere of collective anxiety and uncertainty. This creates a breeding ground for malicious online behavior, with opportunistic fraudsters following spikes in digital activity to ramp up attacks.

Unlike previous inflection points in consumer behavior, triggered by economic events or technology developments, the COVID-19 pandemic has brought dramatic change at an unprecedented speed and scale. With consumer behavior in flux and fraud attack rates rising 20% since the beginning of the crisis*, businesses need to act fast to ensure they are prepared for the rocky road ahead.

* Data from the Arkose Labs network

# Top 5 Challenges: Securing the COVID-19 Digital Economy

Businesses across all industries are grappling with dramatic changes in consumer behavior and traffic volumes. They must adjust to a new normal, whether it involves a major spike in transactions or a rapid pivot towards moving business revenue online. Companies need to protect their customers and ensure they are supporting secure digital transformation.

01 **Sharp Rise in Fraud Attacks**

Fraudsters take advantage of economic uncertainty and new individuals are pushed into cybercrime.

02 **Unpredictable Consumer Behavior**

Consumer traffic patterns change rapidly, making it harder to differentiate between good and malicious activity.

03 **Exploitation of Vulnerable Individuals**

Increase in social engineering and phishing scams taking advantage of anxiety around COVID-19.

04 **New Attack Vectors Emerge**

Opportunistic fraudsters adapt quickly to widen their reach and maximize profits during the pandemic.

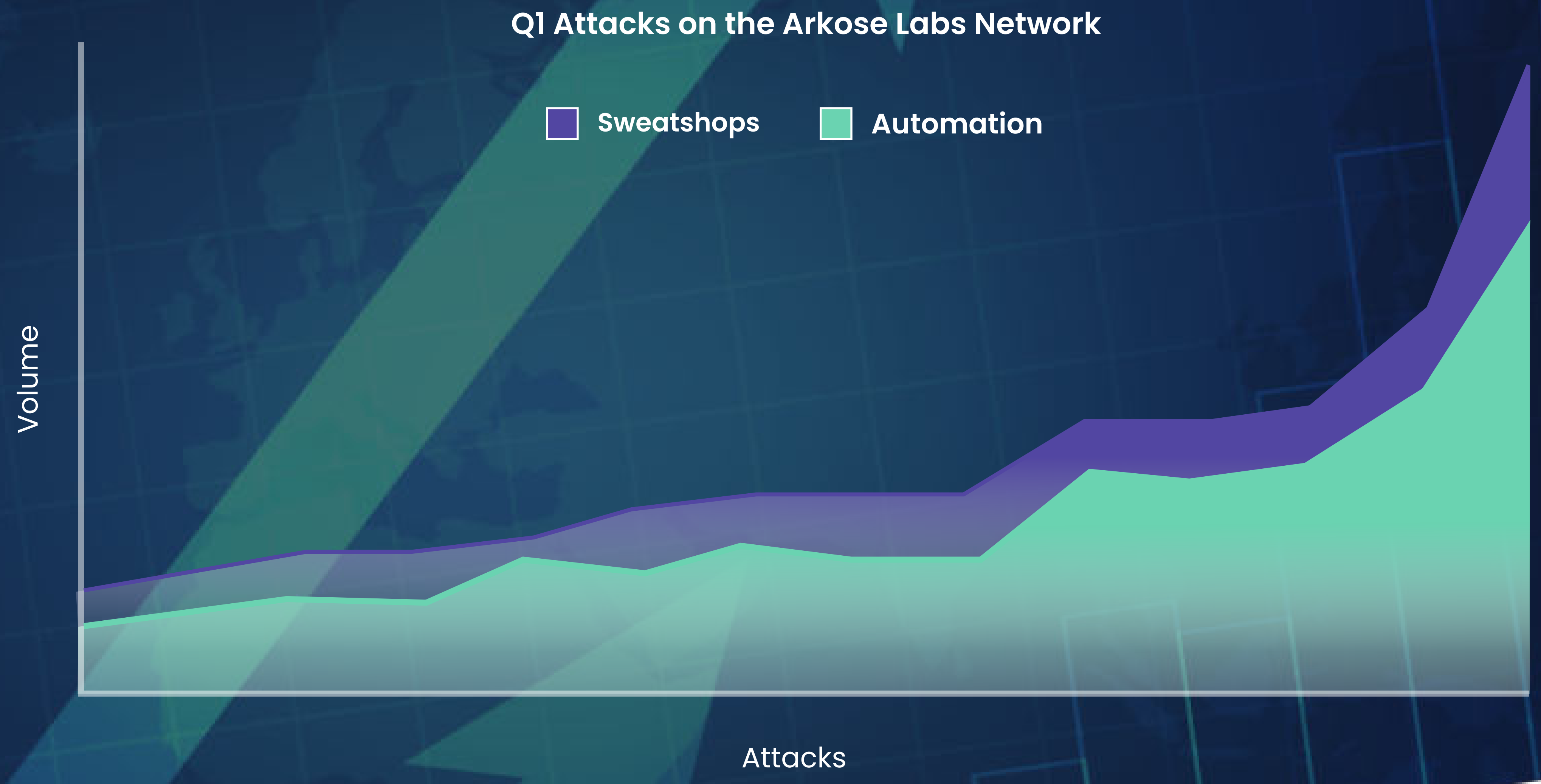
05 **Wider Pool of Sweatshop Labor Available**

Fraudsters move away from traditional fraud hubs to a distributed model of 'guns for hire' across the globe.

# Fraud on the Rise

The COVID-19 pandemic is causing chaos across the world and has cast tens of millions into unemployment. It has already had a major impact on fraud. Attack rates rose by 20% in the first quarter of this year, with payment attacks up by 49% compared to the end of 2019.

Fraudsters are used to adapting to shifts in consumer behavior and anti-fraud technology. They have been quick to take advantage of the current chaos, adjusting their tactics and techniques to quickly ramp up attacks and drive the greatest return on investment from their efforts.



# Fraud in the Time of COVID-19

## Account Takeover

The shift in consumer behavior makes it harder to identify legitimate customers in the face of increasing account takeover attempts.

## New Account Origination

Fraudsters launch large-scale registration attacks, hiding behind spikes in traffic due to the influx of new users on digital platforms.

## Inventory Hoarding

Global shortages of essential items and disrupted supply chains have increased the potential ROI for inventory hoarding activity.

## Spam & Phishing

Fraudsters are ramping up large-scale attacks to take advantage of the crisis and target vulnerable new digital users.

## Scraping

Malicious users are launching high-volume attacks on increased online traffic to harvest identity data and commercially sensitive information.

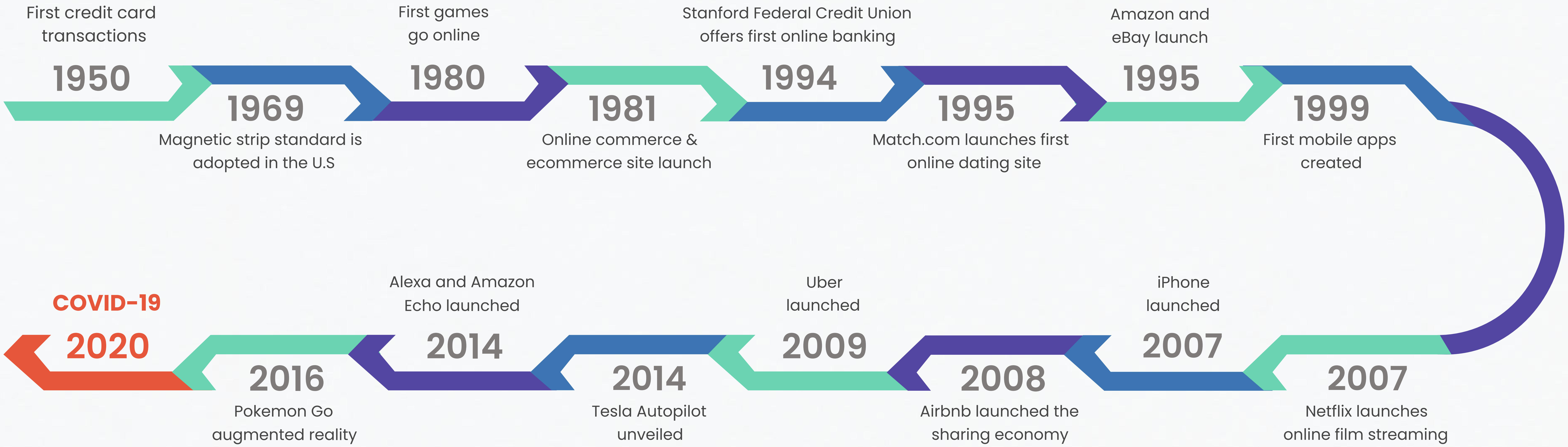
## Payment Fraud

Fraudsters are capitalizing on the surge in online transactions in certain sectors to leverage stolen payment credentials and abuse gift cards.

# A Major Milestone in Digital Economy

**Digital evolution has been driven by tech innovations and disruptive start-ups. Then along came COVID-19.**

The COVID-19 pandemic is forcing industries to rethink the way they operate, as they adapt to the explosion in demand for online services. Even the staunchest technophobes are now accessing the digital economy daily, with both social and professional interactions now happening online. Governments and health agencies are relying more than ever on the internet to disseminate public health information and advice.



First credit card transactions
1950

1969
Magnetic strip standard is adopted in the U.S

First games go online
1980

1981
Online commerce & ecommerce site launch

Stanford Federal Credit Union offers first online banking
1994

1995
Match.com launches first online dating site

Amazon and eBay launch
1995

1999
First mobile apps created

2007
Netflix launches online film streaming

iPhone launched
2007

2008
Airbnb launched the sharing economy

Uber launched
2009

2014
Tesla Autopilot unveiled

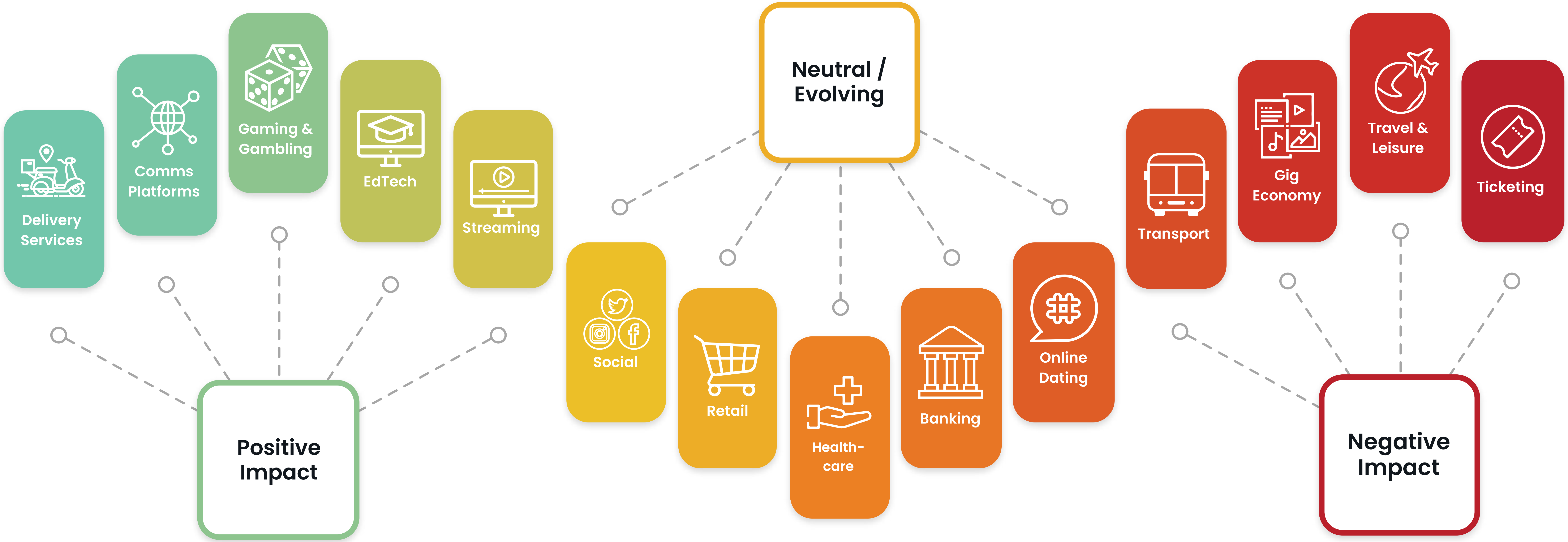
Alexa and Amazon Echo launched
2014

2016
Pokemon Go augmented reality

COVID-19
2020

# The New Paradigm

There will be winners and losers over the course of the COVID-19 pandemic, however one certainty is that businesses across every industry need to fully embrace digital transformation to survive. There will be some short-term upheaval, but this will cause long-lasting changes to the way consumers operate online. Technology adoption is a one-way journey - once digital has become the norm, the average consumer is unlikely to return to old habits.



# Digital Boom for Certain Industries

With consumers currently unable to travel, spend money in physical shops or meet friends and family in person due to social isolation measures, some digital-based industries are flourishing.

**Online Delivery**
Online delivery services have seen an overwhelming rise in demand, with the U.S. grocery industry showing a 100% increase in daily online sales.

**Gaming**
Online entertainment and connectivity are now being seen as essential. A study by Verizon showed video gaming traffic up by a massive 75%.

**Technology platforms**
Individuals increasingly rely on technology platforms for both business and personal activities. Daily users of Zoom have more than quadrupled according to JPMorgan analyst reports.

**Social media**
Individuals are increasingly using social media platforms to connect, communicate and share news stories during isolation.

*https://www.adobe.com/experience-cloud/digital-insights/digital-economy-index.html

# Industries in Flux

Many industries are having their regular ways of operating challenged and are having to pivot to online operations, or deal with major uncertainty and fluctuations in demand.

### Dating

Dating apps are seeing a change in habits as users adjust to an 100% online dating experience. Some are seeing initial dips in traffic but this is likely to be temporary as consumers adopt to new ways of connecting with potential partners.

### Education

Education is traditionally an in-person sector, but with schools closed in 85 countries, the sector is ramping up online services. More than 776.7 million children are now learning exclusively through online platforms.

### Retail and eCommerce

While businesses offering food and other essentials are seeing a massive increase in trade, those selling luxury goods and non-essential items will be at risk as people tighten their belts.

# Industries at Risk

Industries that rely on largely public facing interactions such as travel and entertainment have suffered huge hits already in the wake of the COVID-19 crisis, with estimated losses of 332 billion in stock value over the month of March.

### Leisure and Hospitality

With hotels, pubs, restaurants and tourist resorts closing their doors indefinitely across the globe, online booking services are seeing demand evaporate and stocks plummet.

### Transportation

With bans on global travel in over 90 countries worldwide, the airline industry is among the worst hit, with a projected possible drop in revenues of up to $113bn across the industry**. Local transport is also hit, with Uber seeing reductions of 70% of custom in some cities.***

### Entertainment

Companies and artists alike are in major financial difficulties, as they struggle to navigate the global economic downturn. With no live performances, online ticketing platforms are essentially defunct for the forseeable future.

*https://www.visualcapitalist.com/covid-19-downturn-beach-stocks/

**Projected by The International Air Transport Association (IATA)

***https://www.intelligenttransport.com/transport-news/97647/covid-19-forces-mobility-firms-to-dramatically-scale-back-services/

**20%** increase in attack rate

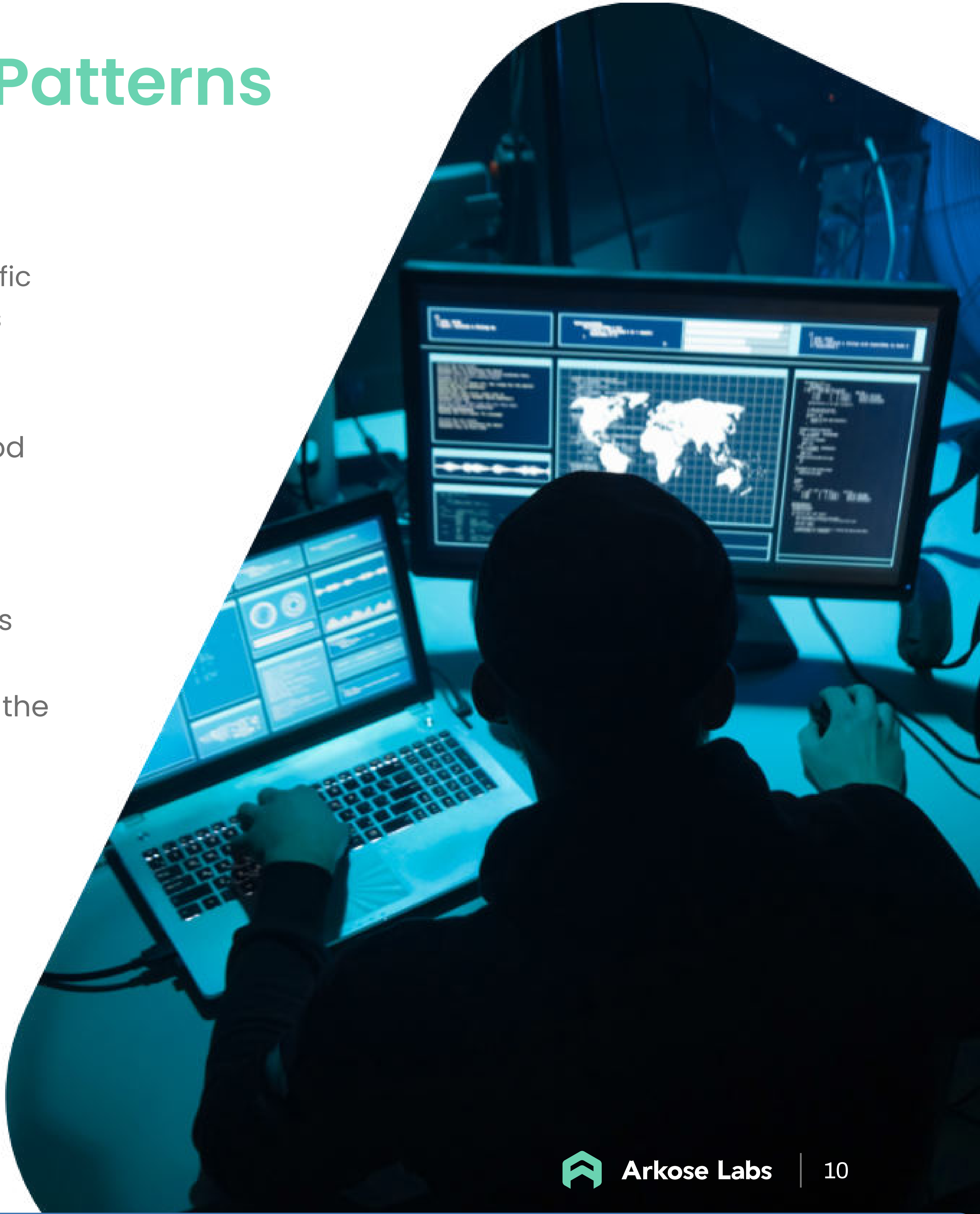
**26.5%** of all transactions are attacks

**445 million** attacks detected in Q1

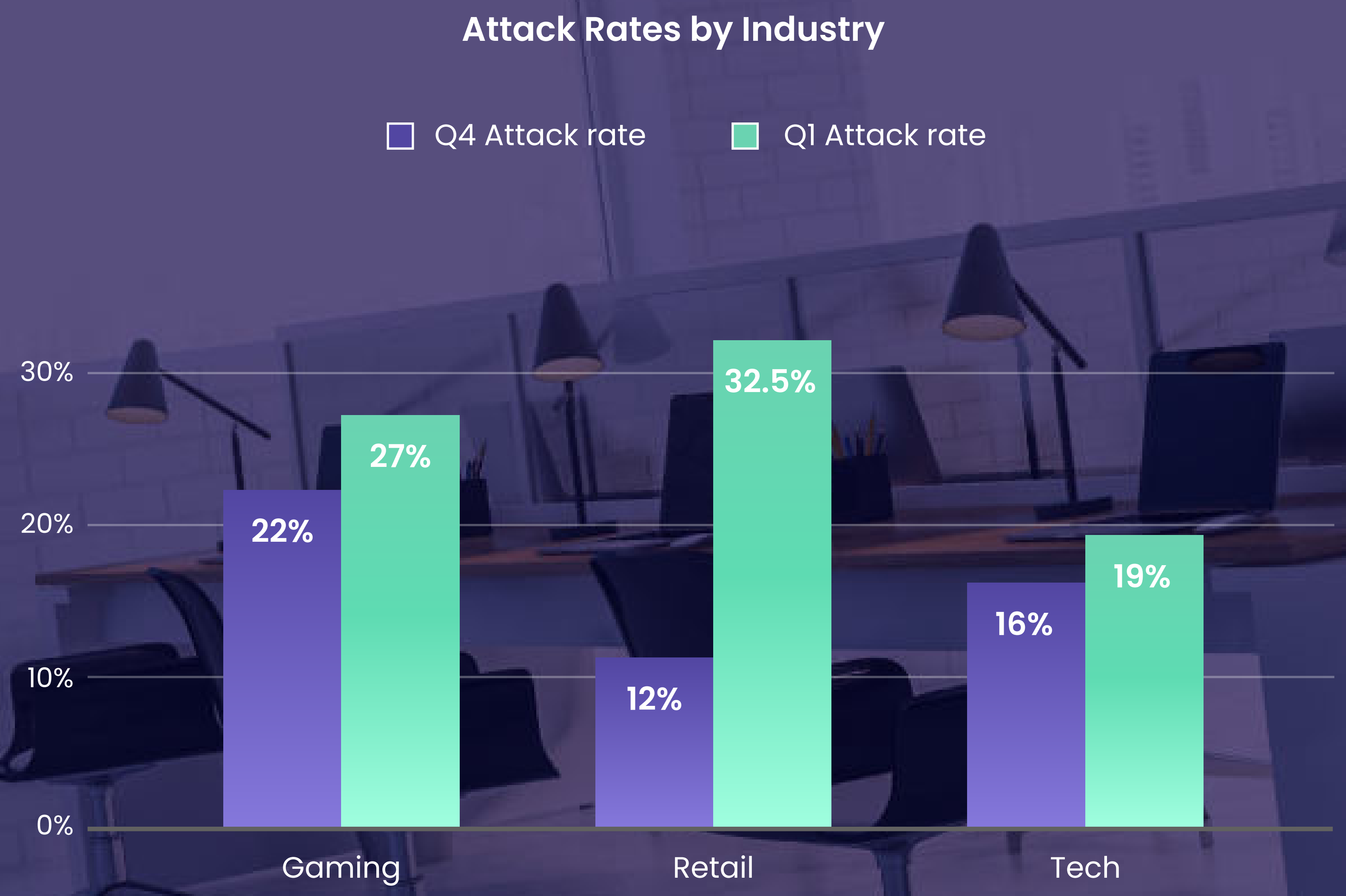
# Changing Fraud Attack Patterns During COVID-19

Arkose Labs has been monitoring the changes in online traffic throughout the crisis. There have been spike in fraud across the network that correlate with increases in user activity.

The first quarter of the year is traditionally a calmer period following the  excesses of the holiday season in Q4. However, COVID-19 is having a disruptive effect, with the first quarter of the year showing the highest ever attack rate on the Arkose Labs' network. 26.5% of all transactions across the network were fraud and abuse attempts. The data predicts that this trend will continue well into Q2 as the COVID-19 crisis continues to cause havoc.



# Top Three Targeted Industries in the COVID-19 Crisis



## 276% rise in attack rate on retail

eCommerce is the top attacked industry during the COVID-19 crisis. This results from the combination of high transaction levels, and an increased risk of inventory hoarding and scraping.

## 23% rise in attack rates on gaming

With a 30% rise in gaming traffic, this industry has become a lucrative target in the new COVID climate. This is primarily driven by automated attacks.

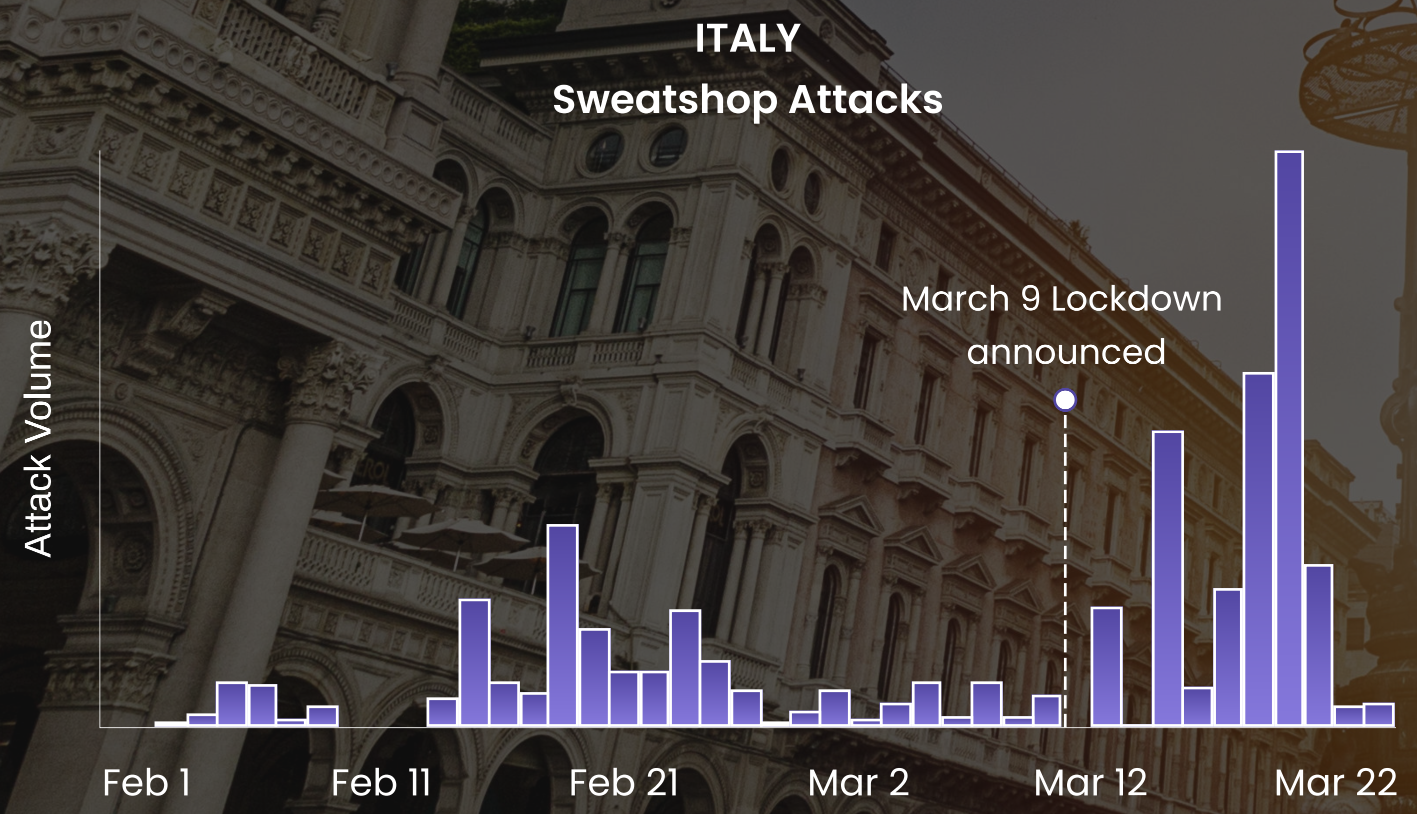
## 16% increase in attack rate on tech platforms.

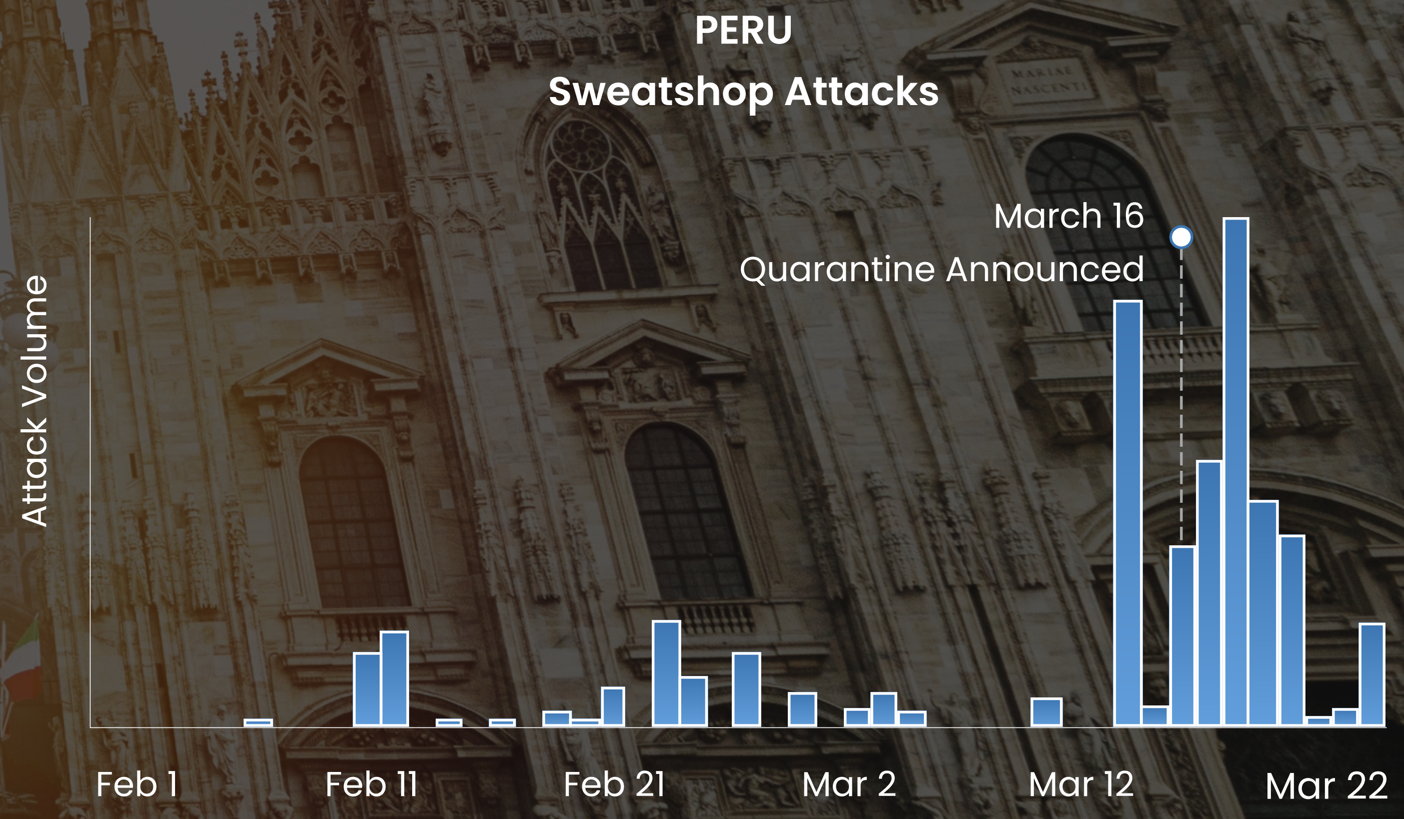
With both personal and professional communications moving online, the increased traffic offers increased numbers of potential victims to fraudsters.

# Lockdowns Cause New Pockets of Sweatshop Activity

Some of the most compelling examples of the effect of COVID-19 can be found in localized data from countries in strict lockdowns. There were immediate spikes in human-driven activity from Italy and Peru directly after the countries implemented social isolation measures.

Fraud has become a fallback career for those experiencing economic hardship. Organized cybercrime outfits mobilize to actively recruit workers, taking advantage of individuals' changed circumstances to maximize profits.





# COVID-19 Scams Abound

The COVID-19 pandemic has given birth to new scams and fraud, tailored to exploit anxiety caused by the crisis.

**Phishing & Social Engineering Scams**

Widespread reports of an explosion in scams connected to COVID-19.

**Misinformation**

Fake medical advice has gone viral across social media platforms.

**Fake Job Adverts**

Bogus offers of attractive packages for key-worker posts.

**Ransomware**

Malicious attacks targeting the health sector and social services.

**Zoom-bombing.**

Hackers access private video chats to disseminate fake information or troll users.

**Sale of Fraudulent or Counterfeit Goods**

Fake listings for PPE and hand sanitizer flourish across online shopping sites.

**Fake Online Communication**

Fake sites created to steal information, with domain names including "zoom".

**Fake Charities or Businesses**

Charities set up to access grants and support.

# Protecting the Vulnerable

The uncertainty created by COVID-19 is causing huge anxiety for many people, leaving them feeling vulnerable and more susceptible to fraud and abuse. Two groups who are especially at risk are the elderly and the young.

Though 67% of over-65s in the USA now use the internet in some capacity, many seniors are less digital-savvy than the younger generation, with more limited access to technology. As the elderly are considered a high-risk group for COVID-19 they are increasingly housebound, often forcing individuals to navigate the digital world for the first time.

On the other end of the spectrum, child identity theft is a growing problem. During lockdown children are spending more time than ever online, logged onto digital classrooms, or social media and gaming networks. This is often unsupervised and fraudsters are increasingly seeing minors as easy targets for scams.

*https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html

# Recommendations for Businesses

01 **Re-evaluate** your entire business, looking for areas vulnerable to fraud.

02 **Accurately differentiate** between good and bad users at the first point of contact.

03 **Use secondary screening** alongside risk and behavioral analysis to weed out bad traffic.

04 **Monitor** all customer touchpoints for evidence of fraud.

05 **Act quickly** to stamp out fraud early and stop abuse happening downstream.

06 **Remove barriers** to ensure user-friendly customer experience and authentication.

07 **Apply zero-tolerance** protection to malicious bots to prevent large-scale attacks.

# COVID-19: Driving Digital Transformation

COVID-19 is making digital transformation an urgent requirement for many consumer-driven businesses. There will be lasting and irreversible changes to customer behavior; beyond  the pandemic lockdown period, with individuals conducting more of their daily activities digitally than ever before.

The crisis has given birth to new and unexpected forms of fraud, and volatile digital transaction levels and online behavior make the task of protecting the growing numbers of digital users all the more difficult. With the intensity of attacks on the rise, businesses must quickly reevaluate their resilience levels to protect their businesses and their consumers.

Businesses must take proactive measures to assess where new attack points may emerge across customer touchpoints and invest in fraud protections that naturally evolve with emerging attack patterns. This will avoid compounding the personal hardships brought on by this crisis, by protecting consumers from fraud losses and abuse.

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Its patented platform combines Arkose Detect, a sophisticated risk engine, with Arkose Enforce, which uses targeted step-up challenges to wear fraudsters down and diminish their ROI. The world's largest brands trust Arkose Labs to protect their customer journey while delivering an unrivaled user experience.

Sales: (800) 604-3319

## Offices

**San Francisco**

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

**Brisbane**

315 Brunswick St, Brisbane, Queensland AU