DATAVISOR

DIGITAL FRAUD

TRENDS REPORT 2021

A DATAVISOR SPECIAL REPORT

The events of 2020 created no shortage of challenges for fraud teams. With quarantines and lock-downs looming for much of the year, millions of consumers turned to digital channels to purchase items and conduct business, opening up new opportunities for fraudsters. Online spending reached more than 18% of total retail sales in the first two quarters of 2020, up from **14% in 2019**.

Many businesses shifted to a remote work model, meaning more people were spending more time online without the safety net of a company firewall. The sudden shift left many businesses struggling to cobble together a remote work technology stack, leaving very little time for research, testing, and security best practices. IT departments were left to figure out how to safeguard internal resources via fragmented teams. Good communication became more mission-critical than ever, and call centers, live chats, social media, and email served as important albeit vulnerable vehicles.

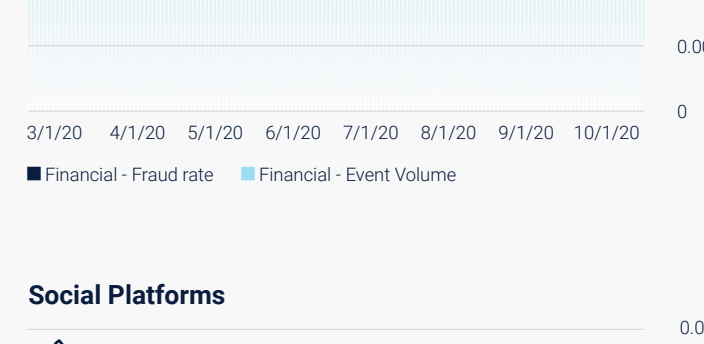
What's more, a heavier emphasis has been placed on mobile technology for consumers, companies, and employees alike. Mobile is increasingly growing in the market, changing everything from how we bank to how we shop. Mobile banking apps account for the third most used app by adults, with more than half of all Millennials having already adopted mobile banking. Mobile technology is also allowing remote work to thrive and helping to keep teams united, as well as serving as a critical line of connection to customers during uncertain times.

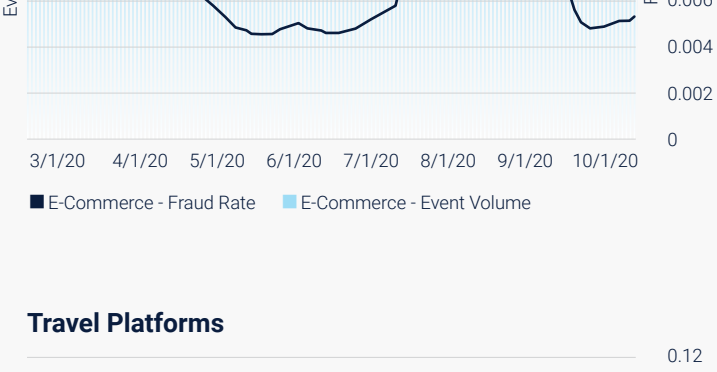
With such major changes in a short time span, it's no surprise that fraudsters were eager to evolve their attacks and exploit gaps in defenses. Using data collected from the previous several months, we can start to understand the current fraud landscape and what might come next.

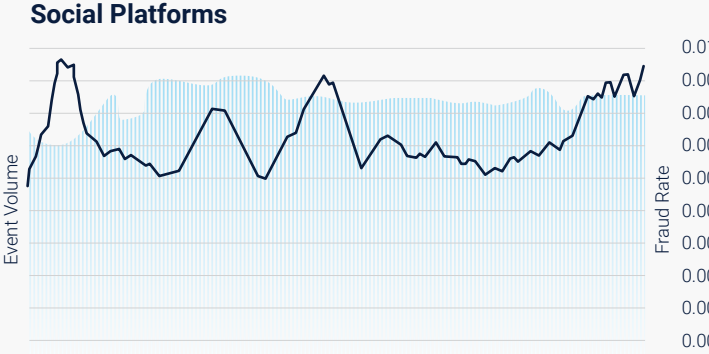
Here's a closer look digital fraud trends from 2020 as we head into 2021:

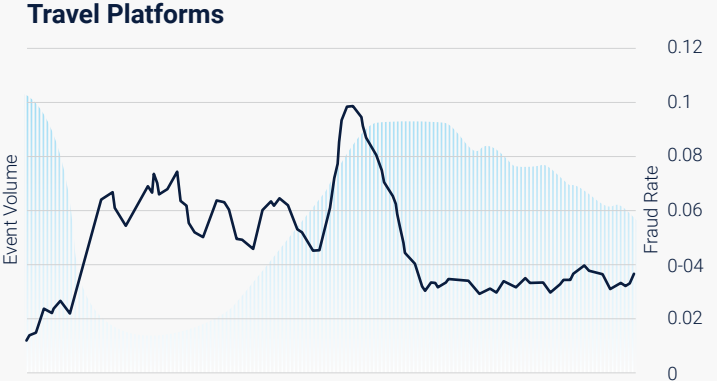
Overall Event Volume and Fraud Rate

KEY TAKEAWAY: Social platform fraud has shown the steadiest growth, traffic volume shows consistent growth across verticals.









We recently reviewed fraud rates and volume across four sectors: financial, E-commerce, social, and travel. The above data reflects a seven-month span from March to October 2020, a critical period of the global pandemic.

After analyzing 128 billion events and more than 2 billion users, DataVisor discovered the following:

The fraud rate on **financial platforms** shows a gradual downward trend after peaking in the spring.

The number of **E-Commerce** events sharply grew between April and June, congruent with the new dependence on online shopping channels for basic staples that may not be available locally. A spike in fraud cases mirrors this uptick in online shopping as fraudsters had more opportunities to commit E-commerce fraud.

Social platforms has seen an increase in events that has held steady for most of the pandemic. A noticeable increase in fraud underscores the importance and vulnerability of social media as a direct communication channel.

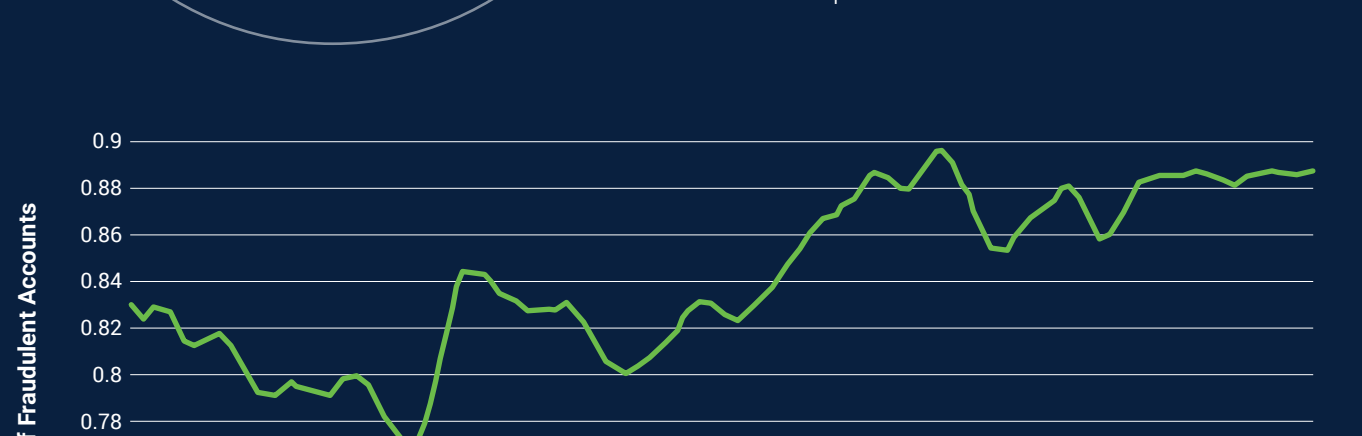
The **travel industry** was hard-hit during the pandemic, but traffic volume recovered in the summer. The fraud rate was high earlier in the year, likely due to the launch of promotional campaigns (anticipating the summer season) and reduced demand from legitimate users.

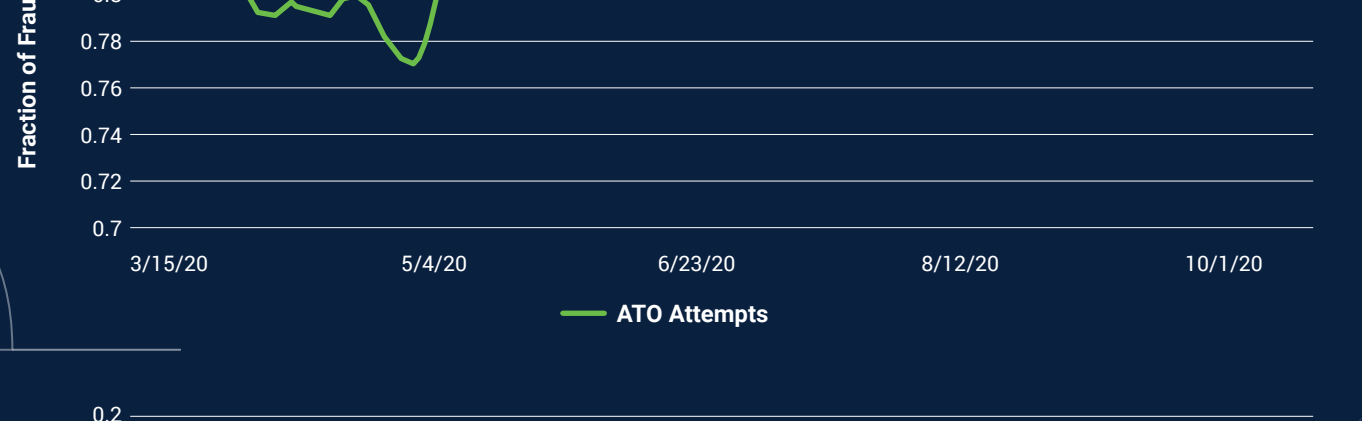
Financial Fraud Attacks

KEY TAKEAWAY: **79-90%** of financial fraud attacks are account takeovers

Among attacks in the financial industry, account takeover is the most common - comprising 70%-90% of fraud attacks. Account takeovers appear to continue an upward trend throughout this year, indicating that this is still an important problem for many financial institutions.

On the other hand, new account fraud and transaction fraud have been trending slightly down, after peaking in the spring when governments around the world issued financial aid and stimulus packages to mitigate the financial impact of the coronavirus outbreak.





Fraud Rates By Channel and Device

KEY TAKEAWAY: Fraud rate for mobile platforms: **0.5%**

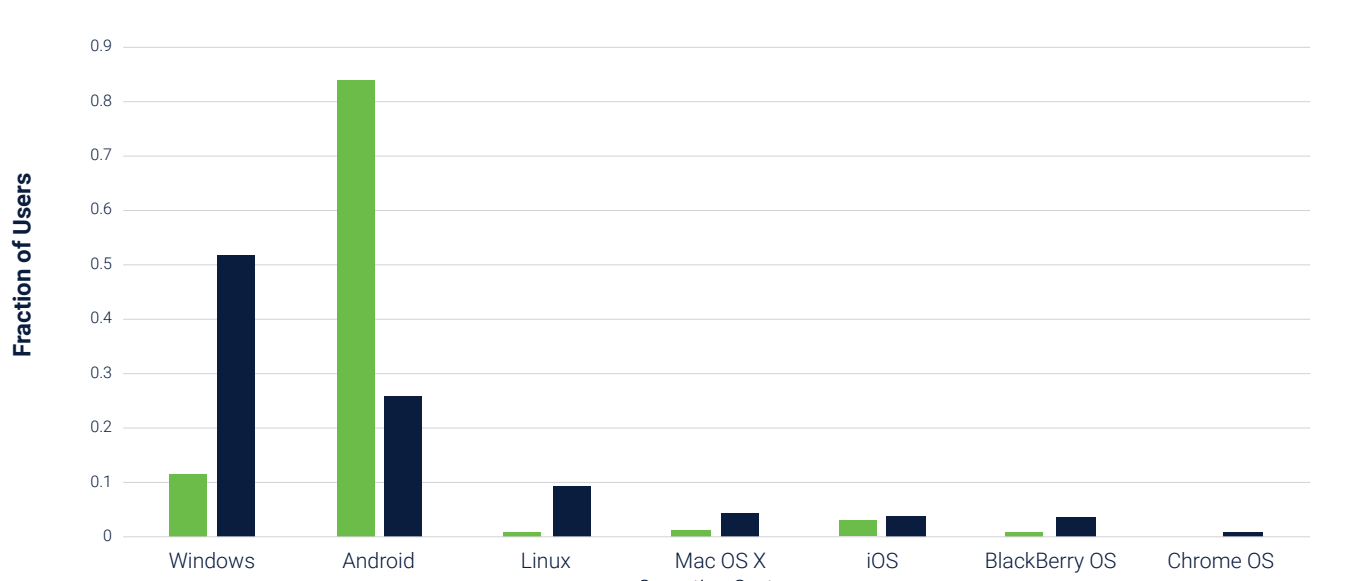
Fraud rate for desktop: **7.4%**

85% of total users are from Android

11% of total users are from Windows

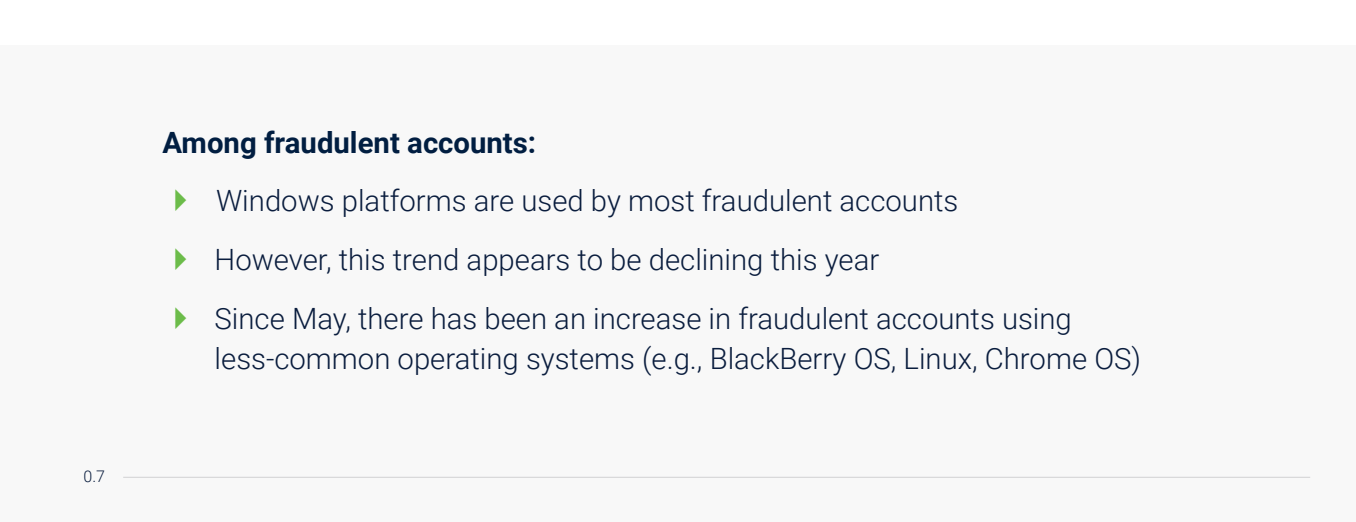
More than **50%** of fraudulent users are from Windows

34% & 26% of user accounts from the web and mobile browsing (respectively) are fraudulent



Among fraudulent accounts:

- Windows platforms are used by most fraudulent accounts
- However, this trend appears to be declining this year
- Since May, there has been an increase in fraudulent accounts using less-common operating systems (e.g., BlackBerry OS, Linux, Chrome OS)



Evolving Fraud Attack Techniques

KEY TAKEAWAY: **22X** more events occur via rooted or jailbroken devices.

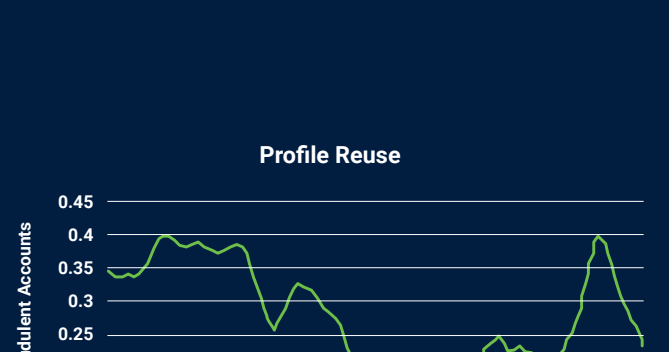
Device Manipulation

Device manipulation is the use of spoofed or emulated devices to carry out fraud. This is a common technique across all verticals and is considered an advanced attack because it may bypass device fingerprinting.

An attack wave at the beginning of the pandemic saw over 10% of fraudulent account openings launched from spoofed devices.

Emulators that allow fraudsters to create the appearance of multiple, unique customer accounts and devices are most commonly observed when fraud attacks are conducted at scale to maximize illicit profits.

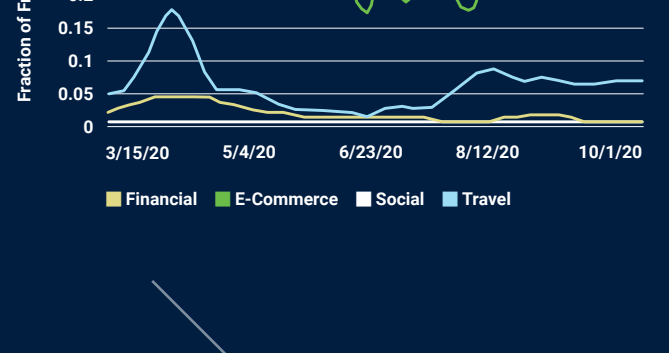
DataVisor research finds that 22x more events occur via rooted or jailbroken devices, both of which appear to be much more active than non-jailbroken or non-rooted devices. This is likely due to fraudsters using them to control multiple accounts at scale.



Low Reputation

A low reputation score is assigned to profiles that have garnered a history of fraud-related activities in the past. This could occur via email addresses, email domains (disposable email providers), IP subnets (proxies, VPNs, data centers), or other digital entities.

Reputation-based fraud detection solutions will never go away, but their utility is limited. Nevertheless, it is a low-hanging effort for catching fraud on financial platforms. At least 4%-6% of the fraud can be captured by examining the category and reputation of digital entities.



Profile Reuse

Fraudulent accounts that share the same identifying information (phone number, mailing address, contact information, etc.) can be stopped with proper profile reuse checking protocols.

This is becoming a major priority for E-commerce platforms that connect potential buyers and sellers since this vertical commonly suffers from scams, spam, and fake listings. In these attacks, fraudsters need to provide valid forms of communication to defraud their victims, resulting in heavy reuse of contact information such as phone numbers and email addresses.

DataVisor research shows that up to 40% of scammers on marketplace platforms reuse phone numbers or email addresses in defrauding their victims (though they may be hidden in images or obfuscated using special characters or similar-looking characters).

Fraud Detection: Human or Bot?

KEY TAKEAWAY: **100%** of fraudulent accounts use automation at some point in their lifecycles, making it harder to distinguish between humans and bots.

One of the biggest questions dominating the fraud landscape in 2020 is: **How many attacks are carried out manually vs. by automated bots?**

Almost all fraudulent accounts are controlled via automated means at some point in their life cycle, including:

- At account registration time (social, E-commerce, marketplace sites), 55% to 90% of fraudulent accounts use scripted names, nicknames, or email addresses
- At least 30% of fraudulent accounts originated from IP ranges associated with data centers, VPNs, or proxies on platforms that experience massive coordinated attacks
- Even on financial platforms, which typically have stricter anti-fraud controls in place (at the cost of higher user friction), we observe that 10% of fraudulent account openings originate from spoofed or emulated devices
- Across all platforms, 40% of fraudulent accounts exhibit "spiky" behavior with sudden rapid succession of activities (a sign of scripted behavior)

Distinguishing between bots and humans is a difficult task. Even CAPTCHAS have a reported **false positive rate** of **8%** (and 29% if the CAPTCHA is case-sensitive).

We are also seeing fraudulent bot accounts successfully bypassing step-up checks: at least **2%** of fake accounts have been confirmed to solve CAPTCHAS, bypassing basic attempts at blocking automated activities.

Emerging Threat: Fraudsters Target MacBook with Apple M1 Chip

In November, Apple's M1 chip was unveiled to the delight of MacBook fans who had been waiting for a faster chip with longer battery life. But there's a problem. The new MacBook equipped with the M1 chip supports running applications on iOS directly. Although this makes it easier to share the application data of the Apple ecosystem, there are also huge security risks, making the M1 chip a perfect tool for fraudsters.

With the M1 chip, all iOS App data running on the Mac is placed in the user directory, and the App sandbox becomes a transparent box. Suddenly, the MacBook is vulnerable to any fraudster who wishes to tamper with the iOS program data. Since the M1 MacBook can run literally hundreds of multiple apps, including iOS apps, it seems likely that this MacBook could become a black market "tool warehouse" for fraudsters.

Fortunately, DataVisor's dEdge, a cutting-edge device intelligence solution, has launched new functions adapted to the M1 chip that:

- Provide reliable DVID (Unique Device ID) on the MacBook
- Provide local data encryption to prevent random modification of the sandbox
- Effectively identify the running of iOS apps on the Mac M1
- Intercept fraud attacks of simulators on the M1 chip

dEdge mitigates emerging fraud threats and provides protection for applications running on any new devices, including the latest MacBook M1 chip.

Final Thoughts

It's becoming harder - and more critical - to separate fraud from fact. As scammers continue to evolve their attacks, fraud departments and organizations need reliable ways to identify new and unknown threats and react in real time without the need for historic data.

To do so in today's digital landscape requires the ability to create centralized fraud intelligence with multi-layered security, such as device intelligence and user behaviors to create full customer lifecycle protection.

Most traditional solutions are incapable of early, proactive detection, as conventional rules-based systems simply can't respond to real-time evolving fraud. Even once-solid tools are proving imperfect in modern fraud detection, as automation is helping fraudsters bypass tools that once required human intervention.

The best path forward is a solution that breaks down data silos and analyzes multiple channels and data points in real time, allowing companies to respond in the moment and prevent downstream damage. Using a comprehensive multilayered approach to uncover highly sophisticated attacks early and at scale can allow companies to stay ahead of the evolving fraud curve and thrive in the digital economy.

Learn about how DataVisor can help you fight fraud.

SCHEDULE A DEMO

About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform for enterprises. Using proprietary unsupervised machine learning algorithms, DataVisor restores trust in digital commerce by enabling organizations to proactively detect and act on fast-evolving fraud patterns, and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of more than 4B global user accounts, DataVisor protects against financial and reputational damage across a variety of industries, including financial services, marketplaces, ecommerce, and social platforms.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR