DATAVISOR

Q2 2020 DIGITAL FRAUD TRENDS

The State of MOBILE FRAUD

A DATAVISOR SPECIAL REPORT

Across today's digital economy, there exist multiple channels by which individuals engage with businesses online. While in-person visitation and call centers continue to play a role in connecting businesses and their customers, digital channels—particularly mobile apps and browsers—are increasingly the primary vehicles for customer experience.

In the financial sector, mobile banking apps were recently reported to be the **3rd most used app by adults** in the U.S. Millennials, who are predicted to comprise **75% of the global workforce** by 2025, are significant drivers of this transition. Studies from Jumio and Javelin indicate that nearly **half of all millennials** have already adopted mobile banking.

As to retail commerce, it has been reported that online spending reached 16% of total retail sales in 2019, with consumers spending more than **$600B online with U.S. merchants**. According to recent projections, more than **50% of e-commerce transactions will take place via mobile in 2021**.

Across the globe, there are **3.5B smartphone users**—nearly half the world's population. Those users combined to download more than **200B apps**.

These numbers serve to make clear the ongoing rise to dominance of the mobile channel. For fraud teams for whom risks and threats associated with web channels are better understood (having been around for more than a decade), mobile apps unquestionably present a whole new threat landscape. In this special report, we explore challenges and opportunities associated with the mobile channel, and introduce advanced new approaches for addressing modern mobile fraud.

Per-Channel Traffic Volume and Fraud Rates: Web vs. Mobile

Traffic volume and fraud rate comparisons between web and mobile indicate markedly different scenarios. Traffic from mobile is much higher, but fraud rates are considerably lower. Web traffic, on the other hand, is a much smaller percentage of overall traffic, but fraud rates are far higher.

Traffic distribution

75%
of traffic comes from mobile apps

12%
from mobile web (i.e., mobile browser)

13%
from general web (laptops, tablets, desktops)

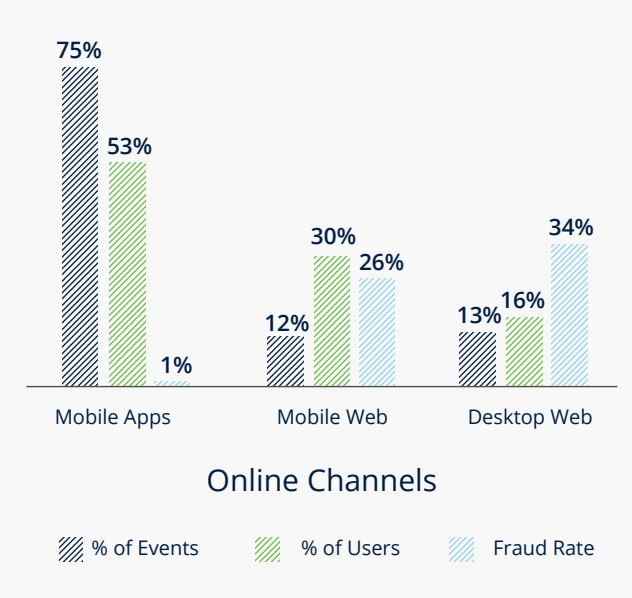

Figure 1:The percent of overall traffic from each channel.

Low fraud rates on mobile can largely be attributed to the fact that the barrier of entry for fraud on mobile apps is much higher. Apps sit directly on devices, and they can collect more accurate device identifiers and monitor user behavior within the app, making it harder for fraudsters to evade detection.

However, there is still cause for serious concern, given that advanced attackers can potentially cause far greater damage while continuing to go undetected.

34% & 26%
of the user accounts from general web and mobile web are fraudulent.

ONLY 1%
of user accounts from mobile apps are fraudulent.

Mobile Channel Fraud Rates by Device and OS

The majority (90%) of fraudulent activities on mobile channels originate from Android devices. Because Android is an open source operating system, malicious users have the flexibility to make system-level customizations and add new features.

90%
of fraudulent activities on mobile channels originate from Android devices.

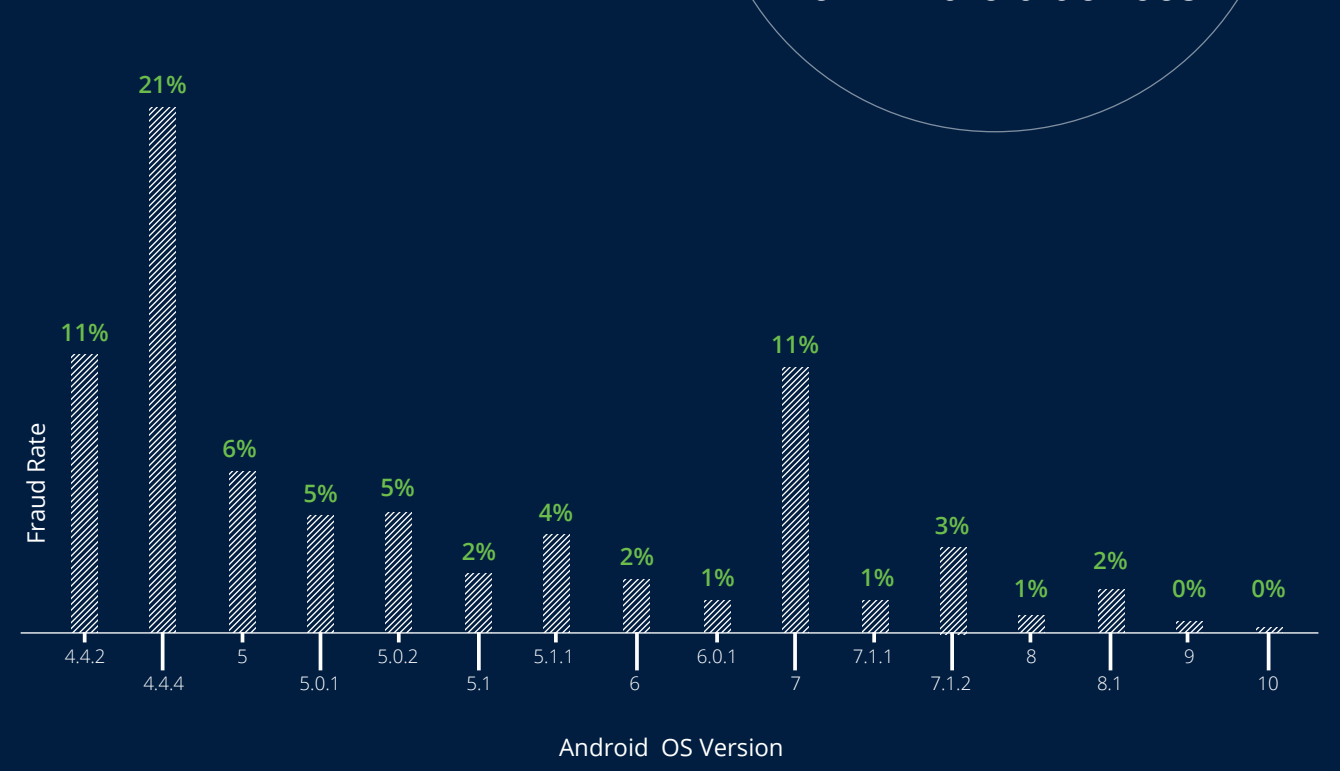

Figure 2: The fraud rate for each Android OS version, sorted by the version release date.

There are also more apps available for Android systems, some of which are specifically designed to spoof GPS locations, forge network requests, automate human-like activities, or provide other functionalities convenient for conducting fraud.

Our data indicates that fraudsters have a slight preference for older OS versions, likely because newer OS versions have security enhancements that make it harder to run hacking tools. Compared to Android devices, iOS devices have a much lower fraud rate. Additionally, unlike with Android, there is no significant difference in fraud rates across iOS versions.

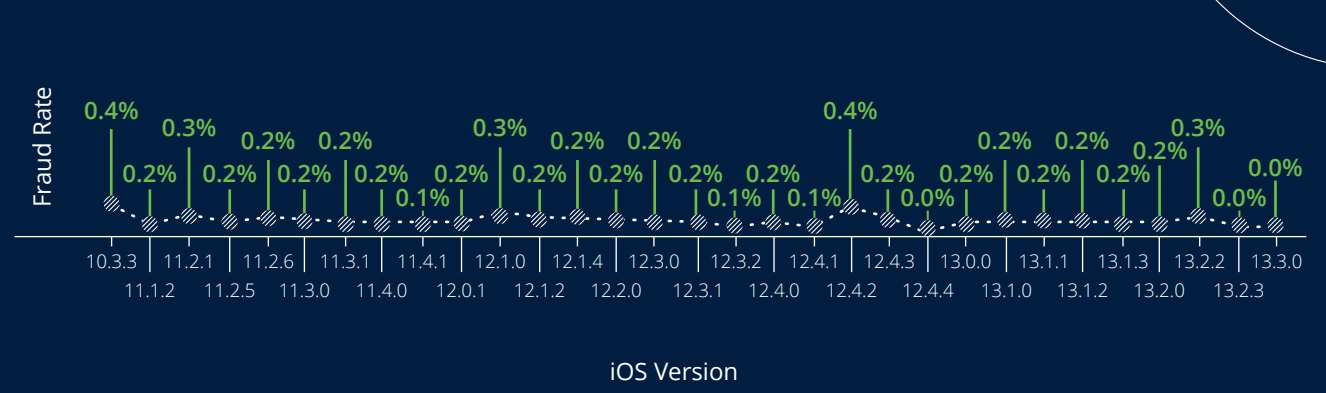

Figure 3: The fraud rate for each iOS version, sorted by the version release date.

Since iOS software updates and upgrades are centrally managed by Apple, the vast majority of iOS devices run recent OS versions. By contrast, we observe a wide range of Android OS versions in use in the wild.

Mobile Threats: Techniques and Tactics

To understand in depth the types of threats associated with the mobile channel, we can measure the comparative prevalence of different fraud techniques used to perform malicious activities on mobile devices, and describe examples of different attack types.

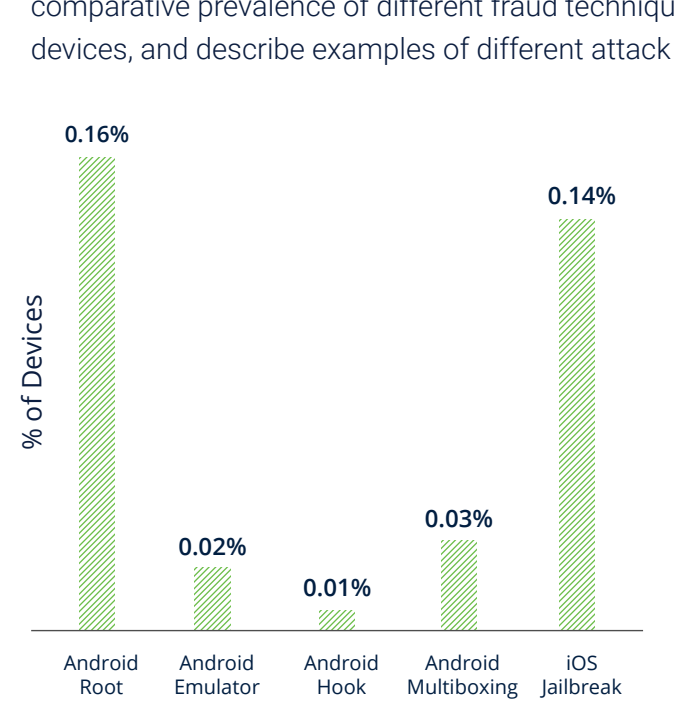

Figure 4: The prevalence of various mobile attack techniques.

0.16% & 0.14%
of devices are rooted / of devices are jailbroken

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.

22x
more events per device are generated in rooted or jailbroken devices than non-jailbroken devices, indicating that compromised devices are much more active, likely due to fraudsters controlling multiple accounts and doing so using automated scripts.

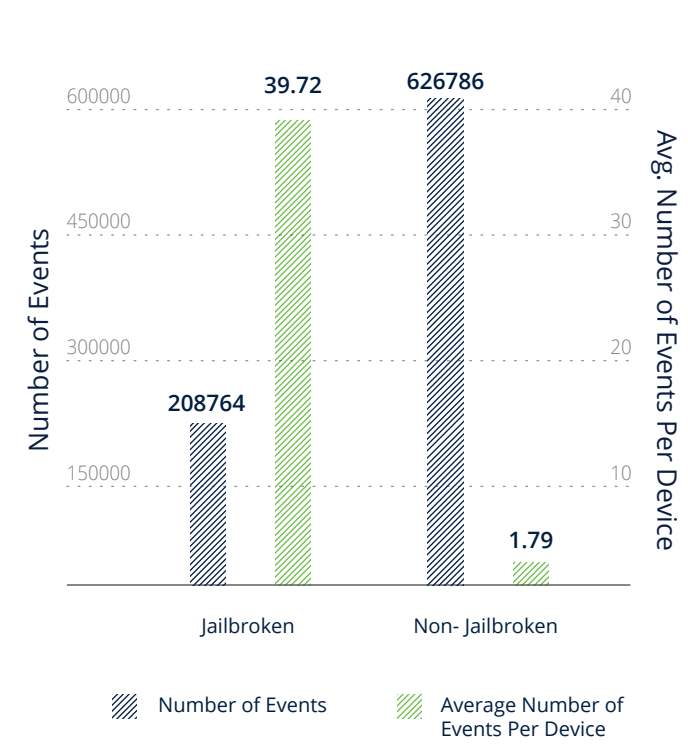

Figure 5: Comparison between traffic volume generated by jailbroken and non-jailbroken iOS devices. Jailbroken phones appear to be much more active, likely due to fraudsters leveraging automation to conduct attacks.

ATTACK EXAMPLES

Emulators and Spoofed User-Agents

The Target
A social media platform

The Attack
Fake accounts created and immediately used to send spam messages

The Evidence

- Accounts all shared the same IP subnet and posted spam messages from the same template.
- Accounts were all created using email addresses from different email domains, with the majority being popular providers like gmail.com, hotmail.com, and mail.ru.
- Every account used a different user-agent string, as collected by the social platform mobile app.
- Each user had a different, random device model, installed with very old Android OS versions released more than six years ago.

Useragent
(melius3g; 4.2.2)
(m0; 4.4.3)
(protou; 4.1.1)
(htc_m8; 4.4.2)
(EBM7000NBD; 4.1.1)
(santos103g; 4.2.2)
(Micromax_A114; 4.2.2)
(S920; 4.2.1)
(u0_cdma; 4.1.2)
(LT29i; 4.1.2)
(ios72_wet_jb3; 4.2.2)
(c8669SA; 4.1.2)
(vee4ss; 4.1.2)
(delos3geur; 4.1.2)
(GT-N7000; 4.1.2)
(SO-02E; 4.2.2)
(cdma_targa; 4.1.2)
(D2303; 4.3)
(d1lu; 4.1.2)
(Auxus; 4.2.2)

Figure 6: Anonymized examples of spoofed user-agent strings likely generated by Android emulators, collected from accounts registered on a social media app.

The Conclusion
This was a coordinated attack using bot accounts controlled through mobile emulators.

Jailbroken Devices

The Target
An e-commerce site with limited-time promotions attracting a high volume of inbound traffic where legitimate requests are inter-mixed with scripts, bots, and fraudulent activities.

The Attack
3000+ fake "users" signed up using VPN IP ranges in China

3.1.0 (iPhone; iOS 11.1.2; Scale/3.00)
3.3.2 (iPhone; iOS 11.3; Scale/3.00)
2.3.1 (iPhone; iOS 11.3; Scale/3.00)
1.5.0 (iPhone; iOS 10.3; Scale/3.00)
3.2.0 (iPhone; iOS 11.3; Scale/3.00)
2.1.0 (iPhone; iOS 11.3; Scale/3.00)
2.4.0 (iPhone; iOS 11.3; Scale/3.00)
1.4.0 (iPhone; iOS 10.3; Scale/3.00)
2.2.2 (iPhone; iOS 11.3; Scale/3.00)
1.3.2 (iPhone; iOS 10.3; Scale/3.00)
1.2.2 (iPhone; iOS 10.3; Scale/3.00)
1.1.2 (iPhone; iOS 10.3; Scale/3.00)
2.5.2 (iPhone; iOS 11.3; Scale/3.00)

Figure 7: Anonymized examples of user-agent strings generated by jailbroken iOS devices collected by an ecommerce site's

The Evidence

- Purchases were sent to fake, non-existent locations.
- All of the addresses followed the same pattern: Random house or apartment number + rotating through a few common road names (Oak, Park, Main) + direction (i.e.. North, South, East, West) + Large city/state
- All users originated from iOS devices that appeared to have installed a wide range of very old versions of the ecommerce site's mobile app.

The Conclusion
Because emulating iOS devices is much more challenging than on Android, it is likely that this attack leveraged jailbroken iPhones, customized for large-scale promotion abuse.

Device Flashing

The Target
A popular mobile game app

The Attack
Fraudsters acted as "brokers" to purchase virtual items on gamers' behalf, leveraging stolen credit cards and virtual currency arbitrage to make a profit.

The Evidence

- Attackers repeatedly logged on as different users to make purchases, without generating any other types of events indicative of actual game play.
- Fraudsters switched out device identifiers frequently—after every couple of users—such that each "device" was only used by a very small number of users, similar to legitimate devices.

EVENT_TYPE	TIMES_DELTA (HR:MIN:SEC)	IP_ADDR	DEVICE_ID	GAMER_ID
LOGIN	00:00:00	23.27.xx.xx	e03107bbd6ce32e7aa5d774312xxx	5342178
PURCHASE	00:00:06	23.27.xx.xx	e03107bbd6ce32e7aa5d774312xxx	5342178
LOGIN	00:08:53	23.27.xx.xx	51a1ead1c71f1384fef9df8d9d5xxx	2390489
PURCHASE	00:00:42	23.27.xx.xx	51a1ead1c71f1384fef9df8d9d5xxx	2390489
PURCHASE	00:01:23	23.27.xx.xx	51a1ead1c71f1384fef9df8d9d5xxx	2390489
LOGIN	00:18:55	23.27.xx.xx	51a1ead1c71f1384fef9df8d9d5xxx	1469185
PURCHASE	00:00:49	23.27.xx.xx	51a1ead1c71f1384fef9df8d9d5xxx	1469185
LOGIN	00:016:51	23.27.xx.xx	0549735007b6d64600e1f463dxxx	2251379
PURCHASE	00:00:16	23.27.xx.xx	0549735007b6d64600e1f463dxxx	2251379

Figure 8: Anonymized example of device flashing used in fraudulent in-app purchases within a mobile game app.

The Conclusion
Device flashing techniques were used by fraudsters to try and avoid raising suspicions about having too many accounts associated with the same device.

Conclusion

Mobile channels generate a significant majority of the traffic that flows to online services and platforms, and mobile apps account for 75% of all traffic. However, while many of the tactics and techniques fraudsters rely on for mobile fraud are familiar—such as rooted and jailbroken devices, emulators, hooks, device flashing, and more—fraudsters are now leveraging automation and vast bot armies to deploy these tactics at massive scale.

It has become increasingly difficult to determine the legitimacy of a given user action or event when viewed in isolation. Scripted registrations blend in effortlessly with thousands of simultaneous new sign-ups. New applications, populated with personal details stolen in breaches and compiled to create authentic-seeming synthetic identities, appear normal in the context of application surges that result from new promotions. Bot-powered fake social accounts build up realistic-looking histories over time before being harnessed to spread scams, spam, and malicious links.

Accurately determining whether users and actions are legitimate or fraudulent requires taking a holistic view of vast amounts of raw data to expose the correlated patterns and hidden connections that indicate coordinated malicious activity. This analysis must be conducted in real time, so fraud and risk teams can confidently make decisions and take action early enough to prevent downstream damage.

A litany of shortcomings renders most existing solutions incapable of early, proactive detection. Conventional rules-based systems can't respond fast enough to rapidly-evolving attack types. Supervised machine learning approaches fail to spot new and unknown threats. A lack of data centralization leaves silos intact, subverting an organization's ability to spot connections between otherwise isolated-seeming instances of suspicious activity.

Threat actors today have the power to cause heavy financial losses to online services through attack types such as account takeover, application fraud, promotion abuse, and more. To defeat them, it is essential that organizations integrate advanced fraud solutions that enable organizations to uncover coordinated, high-sophistication attacks early, and at scale. Only in this way can enterprises stay ahead of threats as our digital economy continues its migration to mobile.

Methodology

To produce this report, we processed and analyzed the following for the period of: **October to December, 2019**

76 Billion
EVENTS

1.3 Million
USERS

4.2 Million
/24 IP SUBNETS

516 Thousand
EMAIL DOMAINS

5.1 Million
USER-AGENT STRINGS

2.1 Million
DEVICE TYPES

The DataVisor Global Intelligence Network

The DataVisor Global Intelligence Network (GIN) leverages deep learning technologies to provide real-time, comprehensive digital intelligence based on a vast set of data signals that include IP subnets, geographic locations, email domains, mobile device types, operating systems, browser agents, phone prefixes, and more. All told, the GIN aggregates anonymized signals across a global client database of more than four billion users. By analyzing the connections between these data points in context—not just in isolation—DataVisor provides fine-grained signals and reputation scores that can be consumed directly in detection, or used to enhance rules engines and machine learning solutions.

info@datavisor.com
www.datavisor.com
DATAVISOR