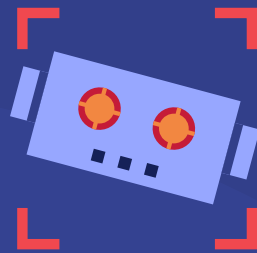


Ad fraud in the app industry.

Why scaling efforts are vulnerable to the effects of invalid traffic.



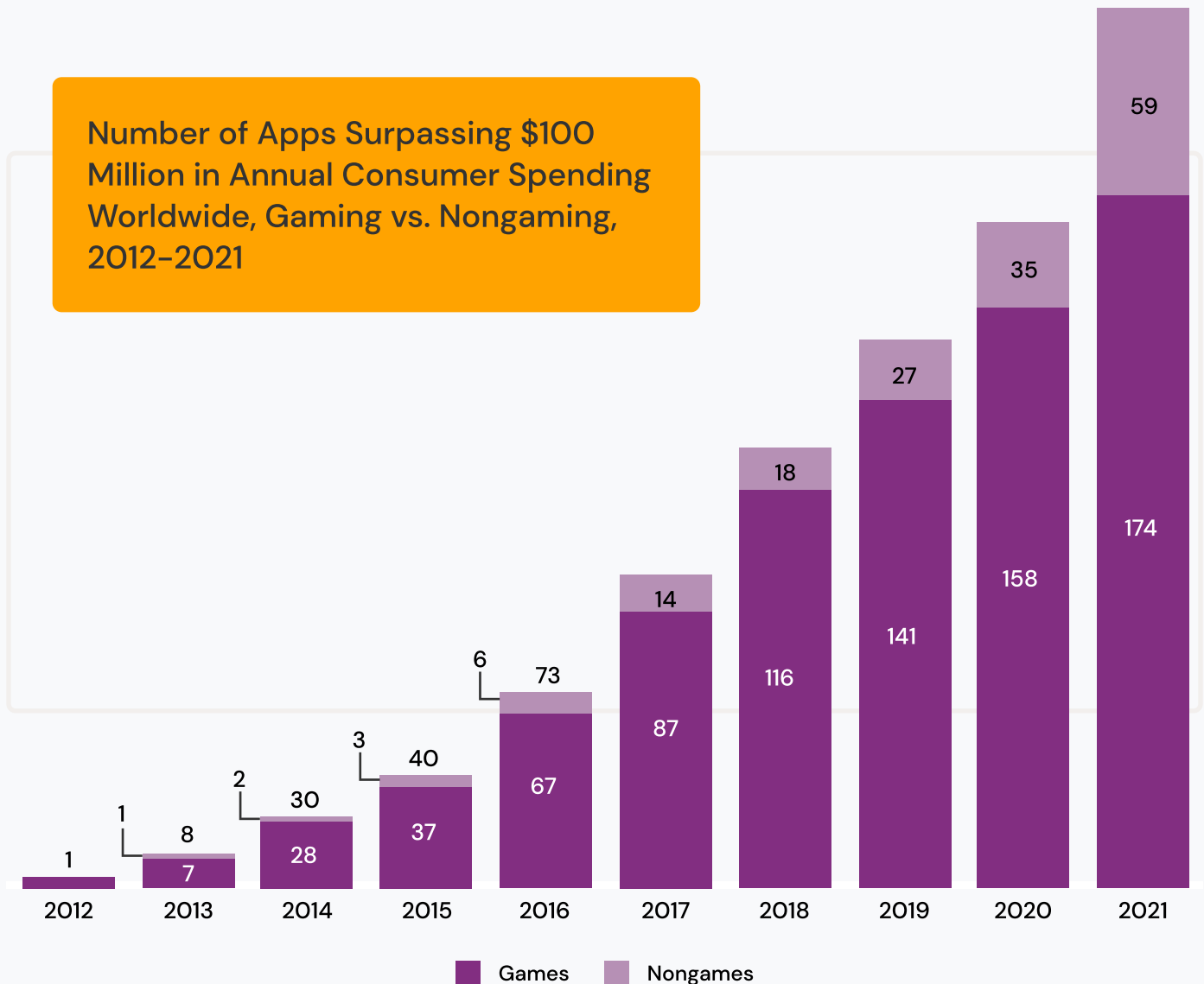
Coming up...

The numbers are going up in the app industry	01
What is invalid traffic?	02
General Invalid Traffic (GIVT)	02
Sophisticated Invalid Traffic (SIVT)	02
How is IVT affecting apps?	03
“I’m using app-ads.txt, aren’t I safe from ad fraud?”	04
Ad fraud in apps: An industry look	05
“No worries here, I’m using an MMP to protect my app from ad fraud.”	06
What’s the risk of not protecting your app’s ad campaigns?	07
The risk of a ‘cold start’ and a lot of wasted resources	07
Scale and risk, a catch 22	08
The misattribution snowball	08
What are the benefits of adopting ad fraud prevention early in an app’s launch?	09
Hit the ground running	09
Supercharge your user acquisition	09
Make your MMP data work harder	09
App case studies: What has TrafficGuard seen?	10
Rappi: How IVT inhibited the growth of a super-app	10
Global fashion retailer: An eCommerce app unknowingly sent poor traffic by their publishing partners	11
Why TrafficGuard?	12
An intelligent solution for an intelligent opponent	12

The numbers are going up in the app industry.

Users are spending increasing amounts of money on mobile apps—both initial downloads and in-app purchases. The past decade has seen consumer spend skyrocket; only one app achieved more than \$100 million annual revenue in 2012, compared to 233 in 2021. The data shows a steady increase year on year, and we can safely predict the trend will continue in an upwards trajectory.

It's great news for apps who clearly have a receptive audience willing to spend big on products and experiences they enjoy. But where big money is exchanged, fraud is always close behind. What dangers do apps face? How are user acquisition targets at risk? How can they protect their increasing revenue? Let's explore.

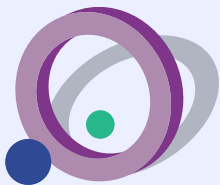


Source: eMarketer, "State of Mobile 2022," Jan 12, 2022

What is invalid traffic?

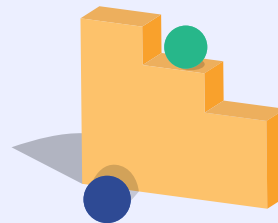
Invalid traffic refers to any clicks or impressions that may artificially inflate an advertiser's costs. IVT is generated by actions that provide no legitimate value to the advertiser, and covers both fraudulent activities as well as accidental clicks—any activity that doesn't come from a real user with genuine interest is invalid.

IVT is segmented into two categories: general invalid traffic and sophisticated invalid traffic. It's worth noting that both types can have a negative impact on ad budgets and performance, even if the IVT is not generated with malicious intent.



General Invalid Traffic (GIVT)

GIVT is the form of invalid traffic most easy to detect. It's usually caused by web crawlers as they index web pages and is not done with malicious intent. GIVT can also come from accidental clicks, and internal traffic.



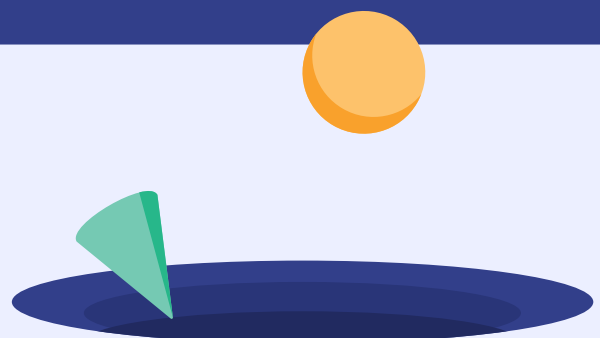
Sophisticated Invalid Traffic (SIVT)

Here's where we'll focus most of our attention. More difficult to detect than its counterpart, SIVT is actively fraudulent traffic created to drain advertisers' budgets and generate inaccurate data. SIVT can come from hijacked devices, adware, competitor clicks, or advertising botnets.



Mathew Ratty,
CEO, TrafficGuard

"Research shows \$1.8–3.6 trillion of capital value erosion is experienced by advertisers globally as a result of ad fraud. These are shocking numbers, and really highlight the urgency that all businesses should feel to safeguard their campaigns against the effects of invalid traffic."

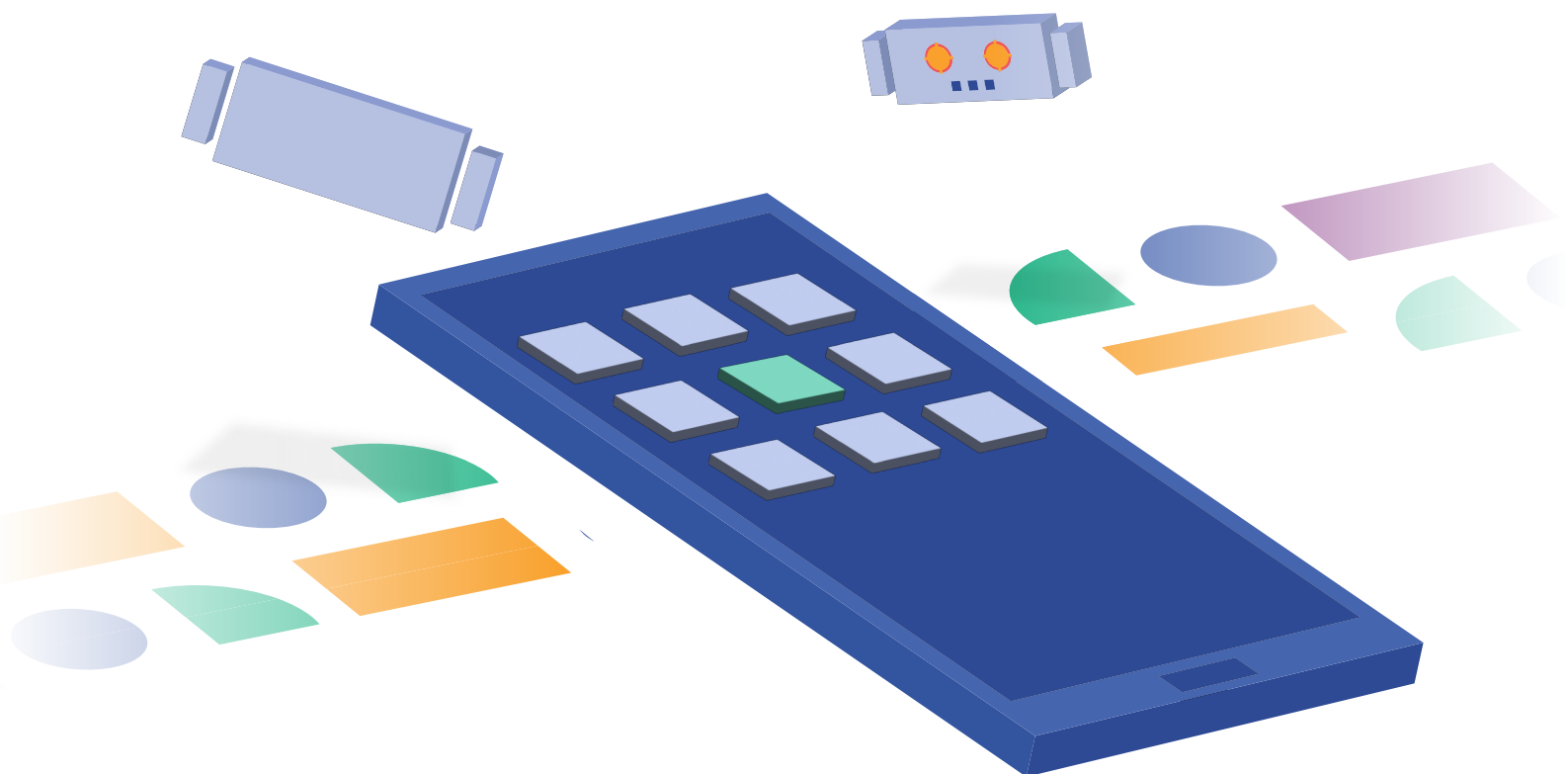


How is IVT affecting apps?

As fraudsters are set to steal over \$100 billion in 2023, marketing teams need to start paying attention to ad fraud. Figures from 2021 show that 7% of app installations on iOS devices were non-human, the same for 12% of installations on Android. Worse yet, there was a 20% post-installation fraud rate from Apple's app marketplace, leading to them removing 170 million fraudulent accounts.

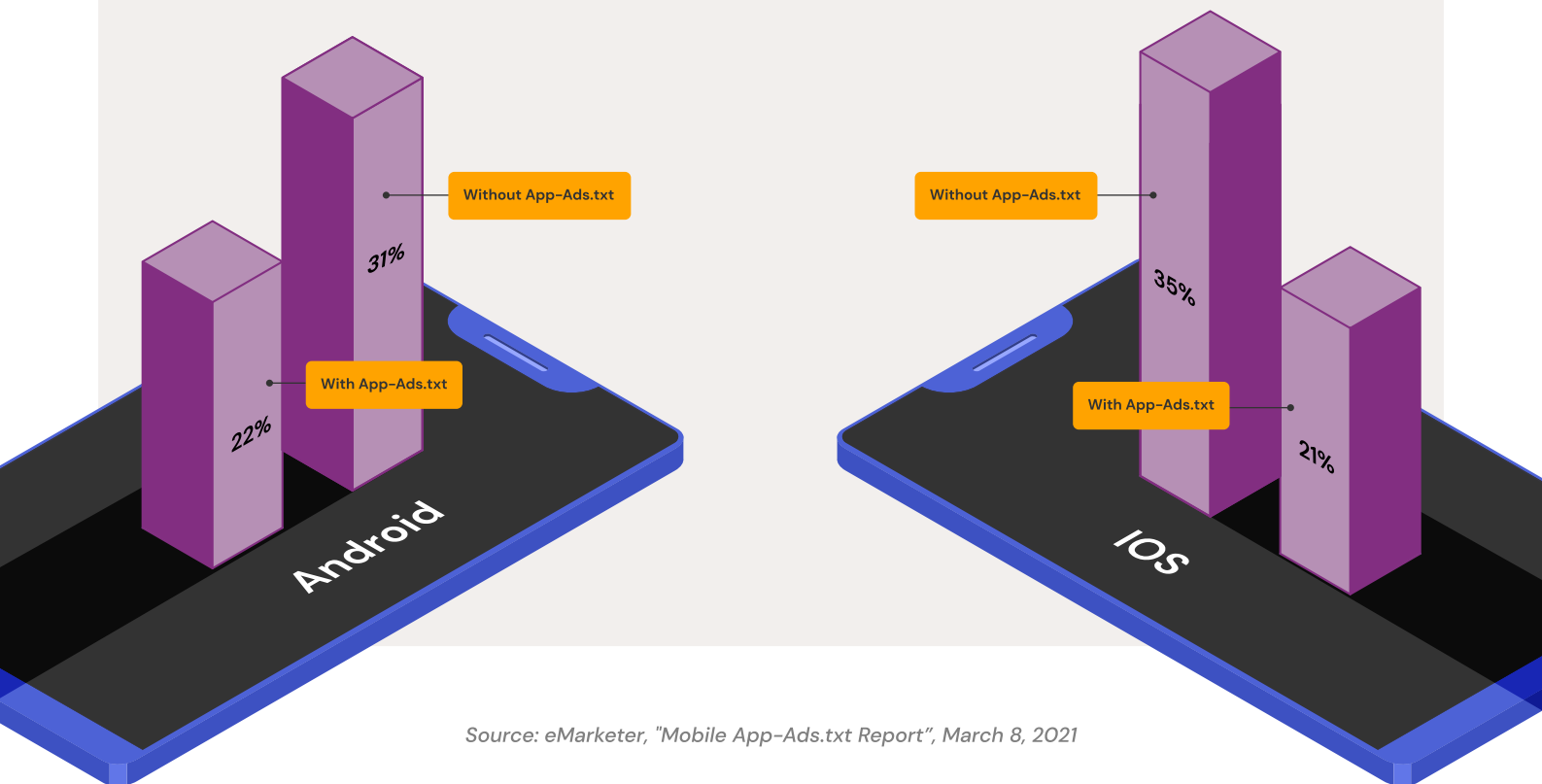
The effects of ad fraud are harmful for any industry, but none more so than mobile apps with ambitious scale plans. Apps are particularly vulnerable to bad actors due to the sheer volume of them out there—even the most conservative estimates put the number at around 8 million globally. That's a lot of apps, with a lot of marketing spend. With so much competition between businesses, many are spending huge amounts on advertising to try and bag the lion's share of downloads and stand out in a crowded market. Unfortunately, fraudsters know this too, and fraud always follows the money.

With millions of apps throwing money and volume at their ads to reach high customer acquisition targets, fraudsters are having a field day pilfering their budgets, and they're going mostly unnoticed. Invalid traffic gets harder to catch the bigger the campaign, which can lead to a cycle of throwing more money at a problem which keeps getting bigger.



“I’m using app-ads.txt, aren’t I safe from ad fraud?”

Programmatic In-App Ad Fraud Rates Worldwide, by OS and Usage of App-Ads.txt, Q4 2020

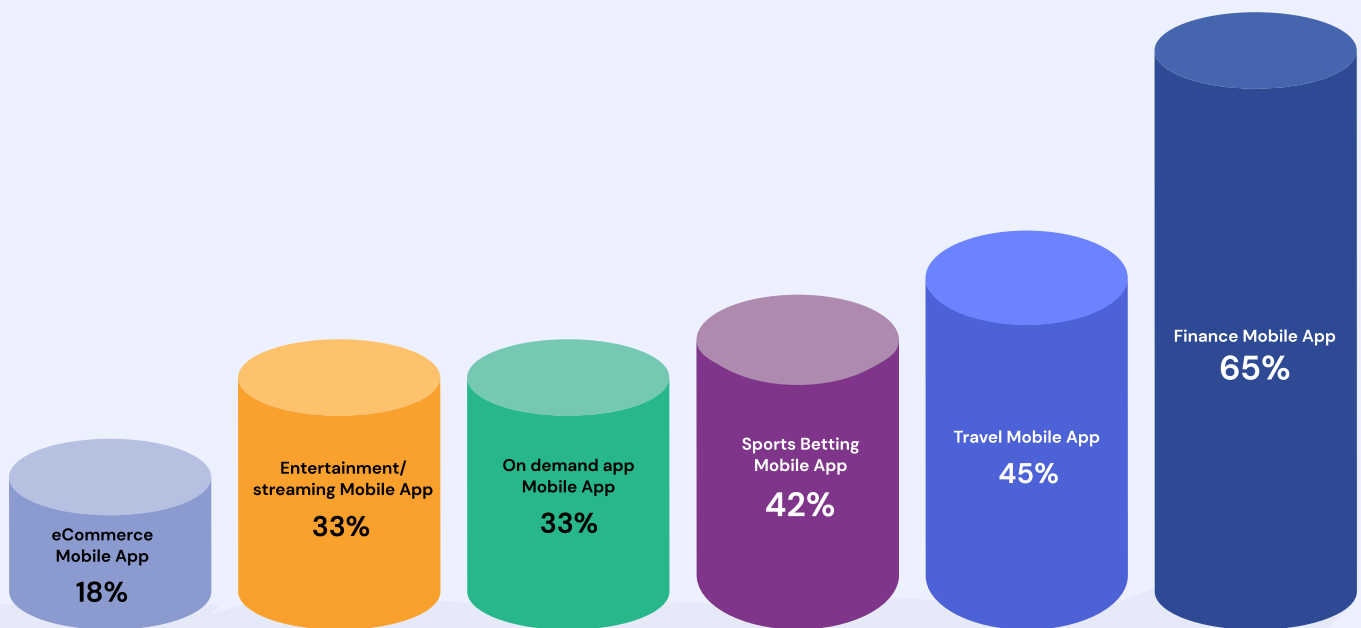


Source: eMarketer, “Mobile App-Ads.txt Report”, March 8, 2021

The app-ads.txt extension was developed to combat domain spoofing by enabling developers to create a list of ad tech vendors authorised to sell or resell their ad inventory on their website. Although apps that utilise the extension experience less in-app fraud rates than those who don’t, the difference is minimal—a trend experienced in both Android and iOS app marketplaces. Clearly more must be done to mitigate the effects of ad fraud within apps.

Ad fraud in apps: An industry look.

Unsurprisingly, apps within the financial sector are hardest hit by ad fraud. The large amounts of money exchanged make the sector a hotspot for fraud, with more than half of installs found to be invalid. Travel is a close second with 45% of installs found to be invalid—mainly due to its large number of high value loyalty programmes which fraudsters attempt to take advantage of. Even industries with lower rates of invalid installs are being badly affected by the effects of fraud, so social and gaming apps should look to protect their campaigns also.



Source: TrafficGuard Platform Data, Sep 26, 2022

It's useful to take an industry viewpoint of fraud as we can identify the sector-specific causes of high rates. However, another class of apps are at particular risk of fraud: newer apps looking to rapidly scale user acquisition efforts.

“No worries here, I’m using an MMP to protect my app from ad fraud.”

Mobile measurement partners (MMPs) provide a valuable service by attributing app installs and measuring campaign performance across advertising channels, media sources, and ad networks. The analytics and tracking provided by MMPs are essential to efficient campaign management; when the origin of the click is known they can calculate return on ad spend (ROAS) extremely well.

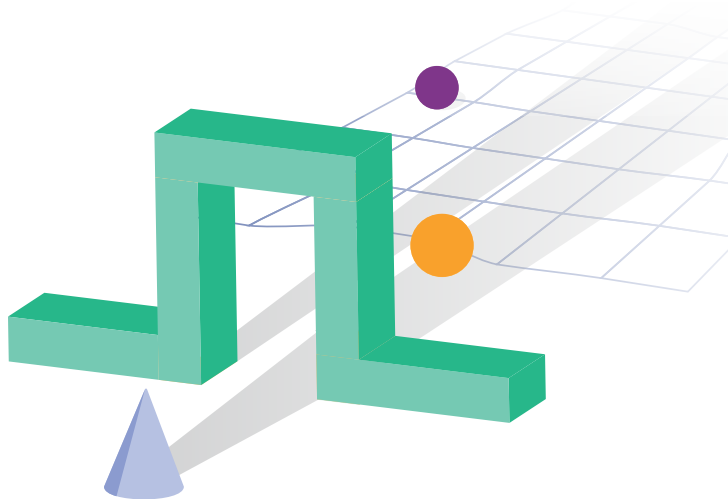
But, crucially, MMPs do not prevent or protect against invalid traffic and ad fraud.

Trusting MMP attribution data alone leaves you open to key vulnerabilities. This is because conventional MMP fraud tools only operate at, or after the app install attribution, not at the impression or click level, potentially distorting attribution data.

To understand why this vulnerability exists in MMP fraud detection tools, we need to take a look at how MMPs operate.

MMPs attribute installs to correct clicks. If there is no ad click associated with the install, the MMP will assume this is organic. If a user clicks on multiple ads over time, the final click before the attribution will be the “winner” and can claim the click and subsequent reward—this process is known as last click attribution.

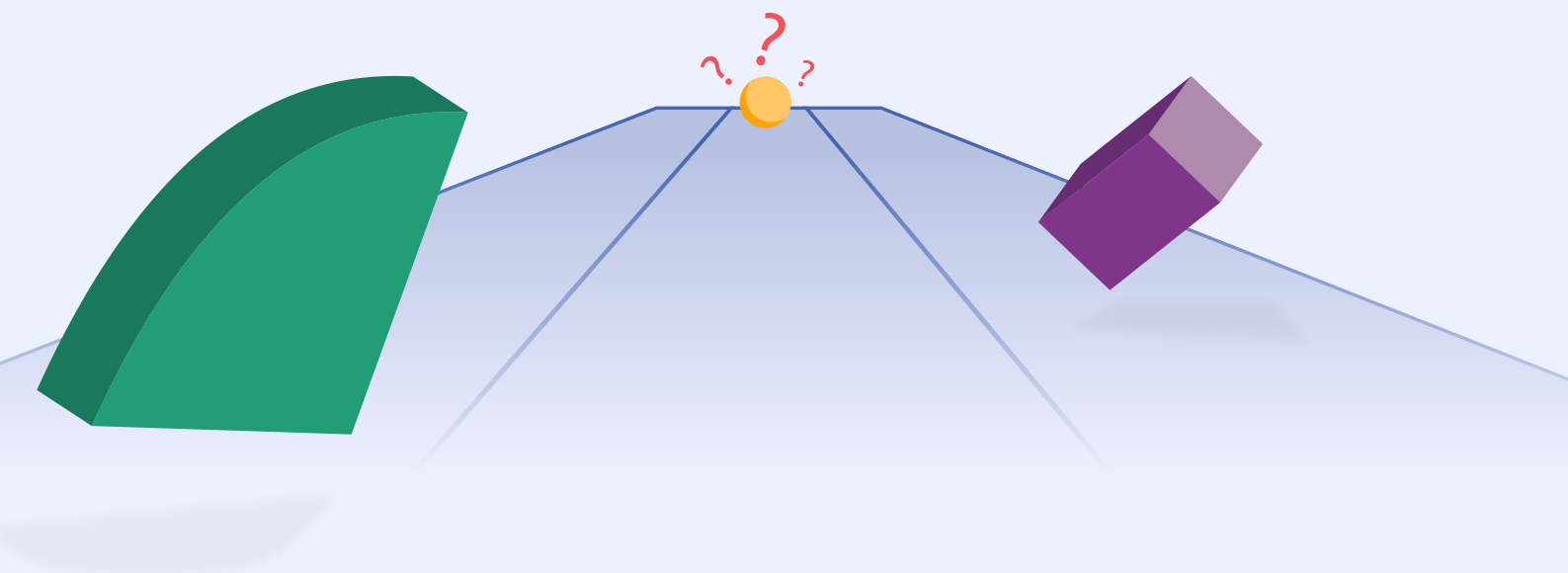
Fraudsters can easily manipulate this system to fool MMPs into attributing them as the click provider, and can subsequently claim the rewards for delivering the clicks. This renders attribution inaccurate, misleading, and inactionable. It defeats the point of having an MMP in the first place.



What's the risk of not protecting your app's ad campaigns?

Many app marketers have ambitious user acquisition (UA) targets to meet. It's often the most important metric within the industry as, obviously, more users = more revenue. Apps with a heavy focus on UA targets, and those with ambitious scaling plans, are at a higher risk of feeling the effects of IVT. Here's how bad actors can hamper growth ambitions.

The risk of a 'cold start' and a lot of wasted resources.



Maybe you're aware of the dangers of ad fraud, but are willing to look past the threat in order to get your marketing efforts up and running. Or maybe you're an ad fraud sceptic, and are waiting until you can see the negative effects on your campaigns before getting protected. Red flag!

If you don't put preventative measures in place before starting or scaling your marketing efforts, it'll be too late to save the validity of any data you collect from your campaigns. Your metrics will be muddled, channel data skewed, and it's going to be really (really, really) expensive to fix.

This mistrust in advertising partners and channels is damaging for relationship building, and the frequent chopping and changing of traffic sources is detrimental to campaigns.

Every time a channel is upheaved, the entire campaign has to start from scratch. That's every bit of work from the ad copy, to the audience research, to the benchmark figures straight in the bin. This makes for some pretty unhappy marketing teams—and even worse results.

We call this a 'cold start'. This can massively inhibit growth, and puts optimisation efforts and insights back to zero. This risks wasting precious investment money.

IVT leads apps to pay the wrong partners, and scale the wrong networks.

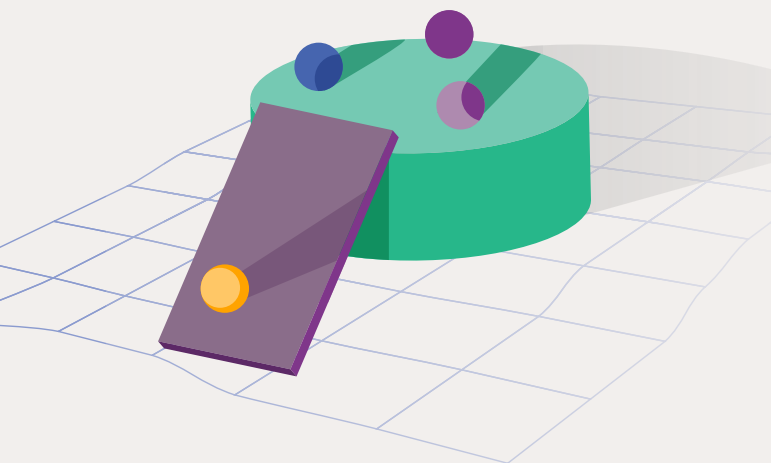
Scale and risk, a catch 22.

Ambitious app businesses know that leveraging multiple advertising channels is the key to boosting user acquisition. To get the best chance of boosting user numbers is to advertise across social channels, UAC (Google's Universal App Campaigns), and advertising networks. Using a combination of channels helps improve UA, and also lowers CPI and CPA.

But (there's always a but), the more channels engaged by an app, the higher the risk of fraud. The more fraud, the worse the results. The worse the results, the more money thrown at the problem. And we soon find ourselves in a cycle of investing large amounts of money into channels delivering poor results because of IVT. This puts a lot of marketers off scaling their marketing efforts.

Getting stuck in this catch 22 situation caps growth and stops marketers taking their campaigns to the next level.

Protection is needed from the word 'go' to give teams the confidence to scale and leverage bigger, better, more lucrative channels.



Misattribution occurs when fraudsters make it appear a channel is delivering more value than it really is, and this has a snowball effect on your performance. A single install attributed to the wrong source will inflate the value of that source not just by one install, but by the value of all the subsequent events of that new user.

Without a reliable understanding of the traffic's quality, there is a risk that campaigns will be scaled with sources that are delivering a high proportion of fraudulent installs. This puts the overall success of a campaign at a huge risk of poor performance. Poor insights can also lead marketers to underinvest in the channels that deliver the best results, restricting their advertising ROI.

The misattribution snowball

💡 **Did you know:** 20–40% of all app installs are invalid or attributed to the wrong partner?

What are the benefits of adopting ad fraud prevention early in an app's launch?

Building a clean ecosystem around your app based on verified, accurate data.



Hit the ground running

The best marketing campaigns are built on verified, accurate data. Launching and growing your app with ad fraud protection means your marketing data is as strong as possible from the word go. This saves your marketing team time and resources as work doesn't have to be redone, and also means not a cent of your investment cash is wasted on fraudulent, irrelevant, unverified traffic.



Supercharge your user acquisition

Layering ad fraud protection across all your campaigns is the only way to hack the risk/scale trade off we spoke about earlier.

Verifying every advertising engagement blocks IVT from campaigns and ensures every click, install, and subsequent event comes from a user with genuine intent. By removing the traffic unlikely to convert, UA metrics already increase by virtue of the more conversion-ready audience pool.

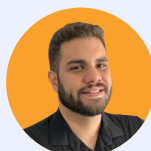


Make your MMP data work harder

Trusting mobile measurement partners' attribution data alone may leave you open to key vulnerabilities, as their anti-fraud tools only operate at or after the app install attribution, not the impression or click level.

Using a full funnel protection solution like Trafficguard as a complement, not an alternative, to your MMP ensures installs are correctly attributed and protected from the effects of invalid traffic.

"As a high growth app, we need to be sure we have accurate and clean traffic in order to keep growing and pushing scale. What we had before was measurement. It was pretty much useless because it limited optimisation and also meant that the more sources we had, the more time-consuming fraud management became. We wanted prevention."

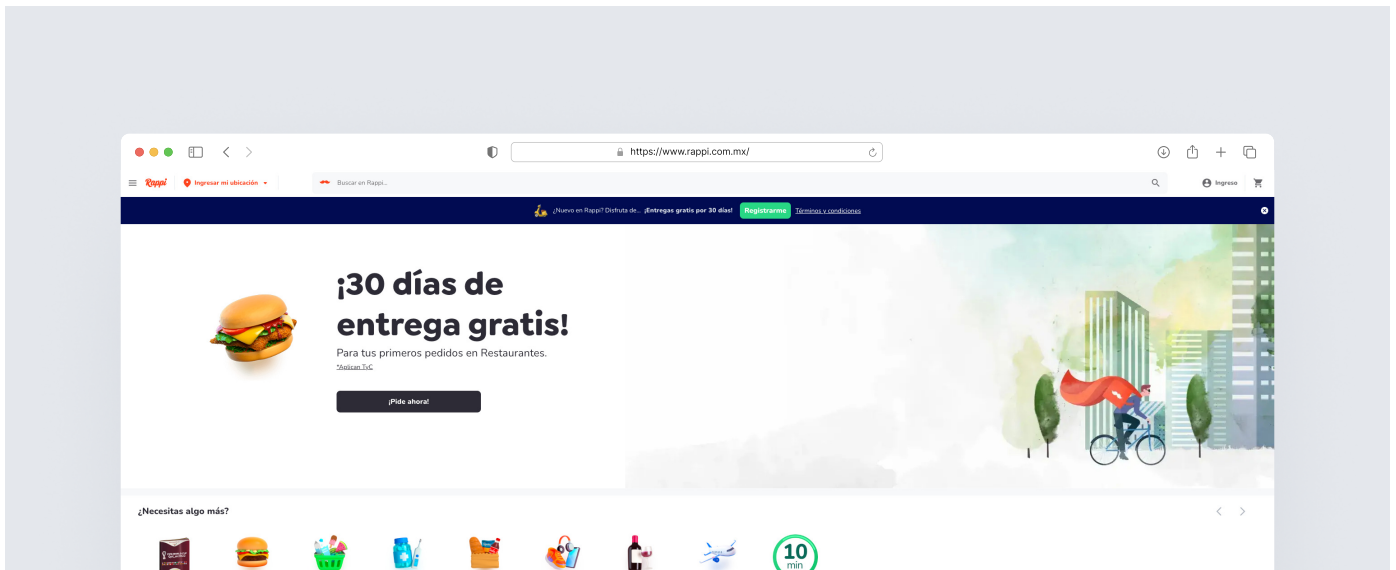


Gabriel Sampaio,
Grow lead-Digital Channel,
Rappi

App case studies:

What has TrafficGuard seen?

The proof is in the pudding. Here's what went down when two different app businesses enlisted TrafficGuard's help to combat ad fraud and improve marketing results.



Rappi: How IVT inhibited the growth of a super-app.

Brazil based on-demand delivery app Rappi was focused on rapid growth, an already difficult task in a crowded market.

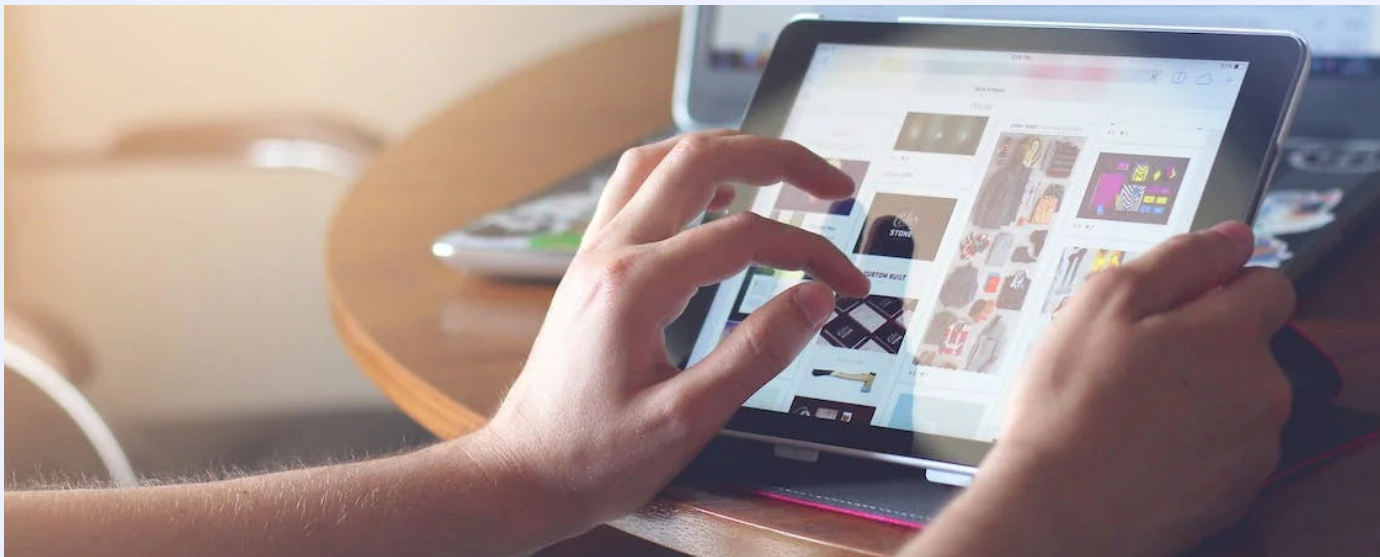
Ad fraud was affecting the business in many ways, some of the worst effects included:

- High, volatile click volumes which made traffic analysis difficult.
- Low conversion rates, despite those high click throughs.
- A huge drain on resources, they estimated 30% of the growth team's time was spent manually analysing and cleaning data of ad fraud for optimisation.
- A growth inhibiting scale/risk trade off.

What about the numbers? During their audit period, TrafficGuard:

- Invalidated 25% of Rappi's clicks before attribution could occur.
- Gave the growth team back 30% more time by mitigating the need for manual data cleansing.
- Improved ROI by 25% due to a reduction in wasted ad spend.

App case studies: What has TrafficGuard seen?



Global fashion retailer: An eCommerce app was unknowingly sent poor traffic by their publishing partners.

This retail app needed verified insights into the traffic being sent by their publishing partners to monitor their investment.

What we revealed? Metrics that would scare any performance marketing manager. Take a look.

- Out of 1.1 billion clicks on their ads, 630 million were invalid. That's a shocking invalid click rate of 57%.
- Of those clicks which became downloads (765k in total), 308k were invalid, creating an invalid install rate of 40%.
- At the post attribution level where we monitor in-app events (that includes items being added to carts or users navigating through articles), 61 million of the 170 million events monitored were found to be invalid—an invalid event rate of 36%.

Why TrafficGuard?



An intelligent solution for an intelligent opponent.

TrafficGuard uses machine learning algorithms to detect and block shape-shifting invalid traffic and ad fraud attempts. Even the most rudimentary fraud tactics can circumvent the rules put in place by legacy vendors, making AI/ML processes not only desirable, but completely necessary for adequate campaign protection.

We use AI/ML models which analyse combinations of indicators over time and across devices to detect fraud as it evolves, as well as mitigate false positives. When used alongside rules engines and blacklists, TrafficGuard's models provide far greater protection against both known and unknown forms of ad fraud.

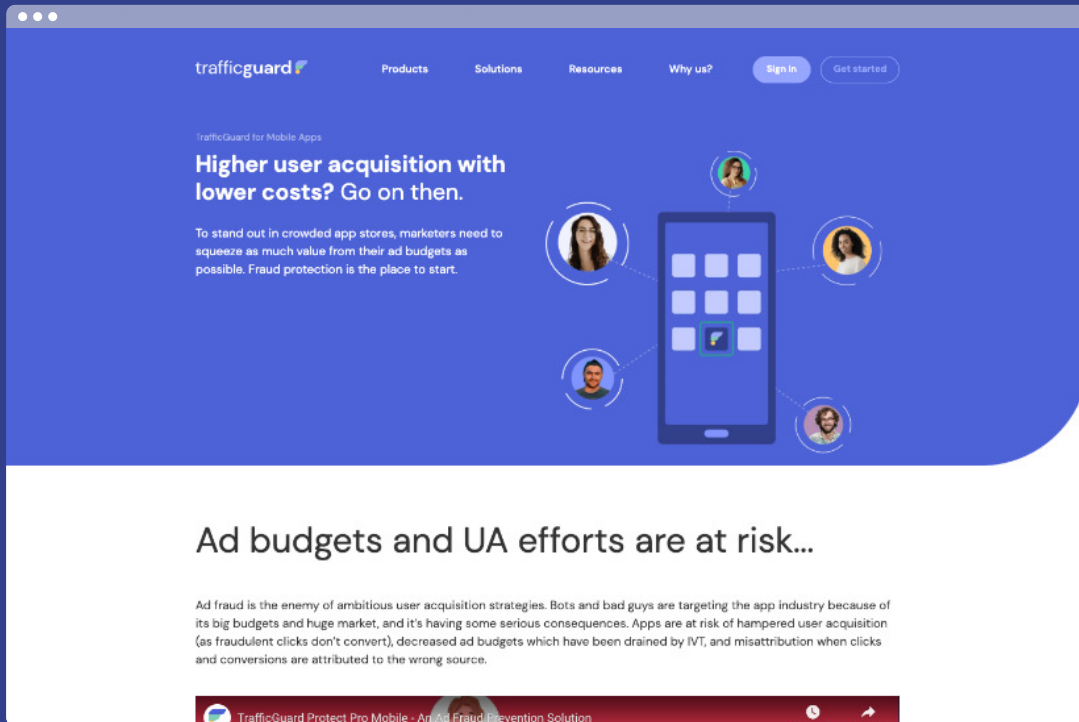



Matt Sutton,
Global CRO, TrafficGuard

"Different apps experience different types of IVT, at different times of day, across different networks. The goalposts are constantly moving, and that's why an AI/ML solution is critical. Plug and play solutions are not sophisticated enough to fully protect campaigns."

TrafficGuard's Got Your App.

Want to know more? Get in touch
over at trafficguard.ai




trafficguard  Products Solutions Resources Why us? [Sign in](#) [Get started](#)

TrafficGuard for Mobile Apps


Higher user acquisition with lower costs? Go on then.

To stand out in crowded app stores, marketers need to squeeze as much value from their ad budgets as possible. Fraud protection is the place to start.



Ad budgets and UA efforts are at risk...

Ad fraud is the enemy of ambitious user acquisition strategies. Bots and bad guys are targeting the app industry because of its big budgets and huge market, and it's having some serious consequences. Apps are at risk of hampered user acquisition (as fraudulent clicks don't convert), decreased ad budgets which have been drained by IVT, and misattribution when clicks and conversions are attributed to the wrong source.

 TrafficGuard Protect Pro Mobile - Anti Ad Fraud Prevention Solution

