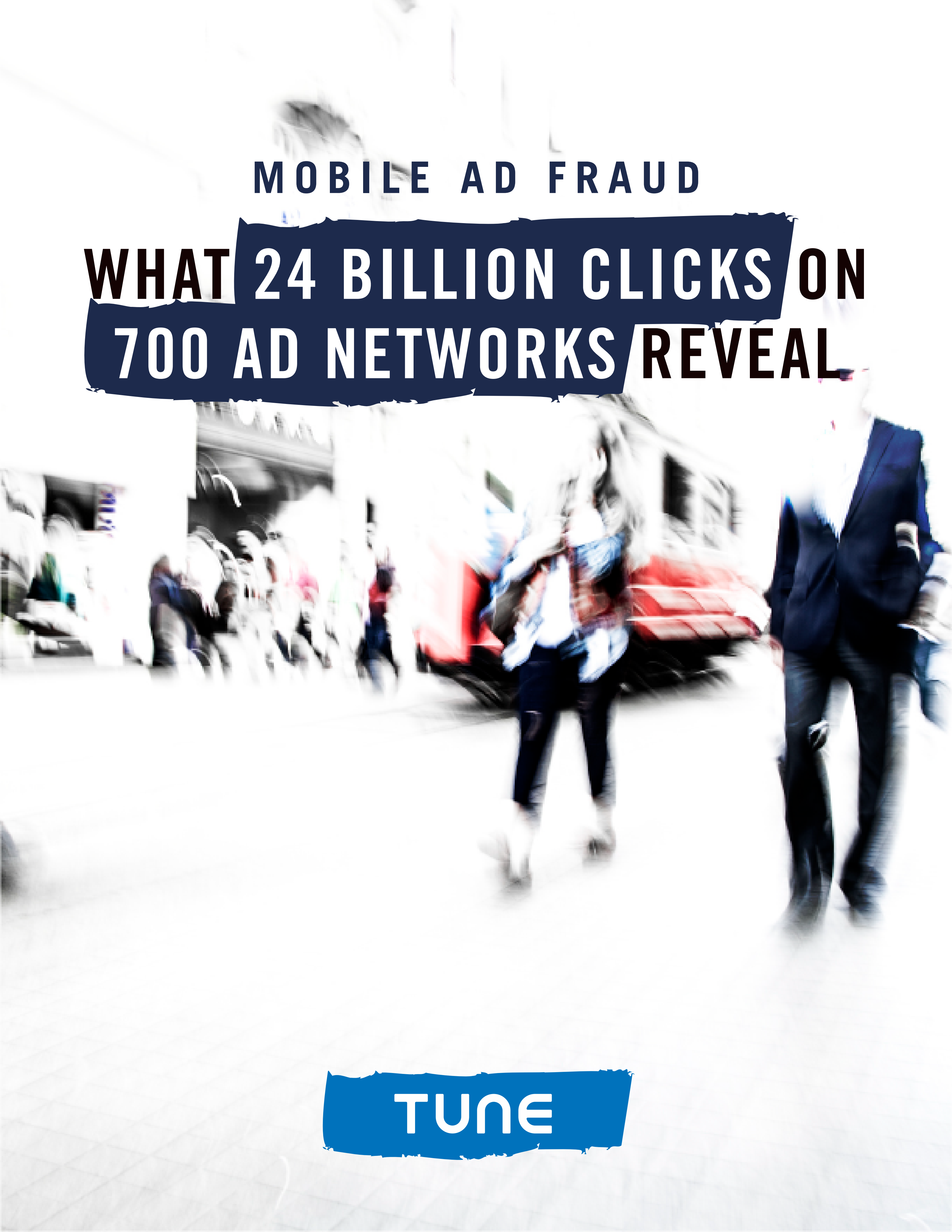
MOBILE AD FRAUD

WHAT 24 BILLION CLICKS ON 700 AD NETWORKS REVEAL



TUNE

TABLE OF CONTENTS

AUTHOR: JOHN KOETSIER

John Koetsier is TUNE's mobile economist. He studies, analyzes, and forecasts trends affecting the mobile ecosystem.

/johnkoetsier johnkoetsier /johnkoetsier TUNE blog

EXECUTIVE SUMMARY

Eight ad networks are 100% fraud.

35 ad networks are 50% or greater.

I recently studied 24.3 billion clicks on more than 700 ad networks, and the results are shocking

If you're marketing on mobile, there are a huge number of ad partners to consider. Some of them are great. Many of them are good. But some are shady characters to watch out for, and the hard truth for marketers is that virtually no ad network is completely untouched by fraud. As a result, marketers must get the proper tools to avoid being cheated.

And, though it may be shocking for defrauded and disillusioned marketers to hear, so do the ad networks themselves.

AD FRAUD: A $16.4 BILLION PROBLEM?

Estimates of ad fraud vary wildly.

One, based on digital security company WhiteOps' data, suggests that marketers **lost $7.2 billion** to digital ad fraud last year. Another, by ad verification company Adloox, suggests that marketers will **lose $16.4 billion** to ad fraud in 2017. Clearly, even if those numbers are off by a factor of two, ad fraud is a massive problem.

A crucial point: This fraud percentage is increasing in spite of huge and widely publicized efforts to eliminate it.

As you'll see, that failure is almost entirely due to structural issues in the way the adtech ecosystem was built … rendering single-player solutions impractical, ineffective, and in fact, almost impossible. Those structural issues are ones that TUNE's fraud analysis technology works to solve.

More than that, TUNE's fraud analysis reporting is the only tool available that solves those structural issues at the source — for both marketers and ad networks — by examining details at the publisher or affiliate level.

On mobile, there are multiple opportunities for fraudsters to make an undeserved buck.

TYPES OF MOBILE AD FRAUD

There are three major types of app install fraud, as TUNE's Marketing Intelligence Manager, Jessica Reichow, outlined recently:

Click fraud: fake click, genuine user

Install fraud: fake click, fake user

Compliance fraud: genuine click, genuine user, wrong user geography/profile/etc.

In addition, there are multiple kinds of non app-install mobile ad fraud, including:

Viewability fraud: stacked, off-screen, not viewable

Targeting/compliance fraud: served to real people, but not the audience a marketer wants

Bot fraud: served to bots or software agents, not real people; the bots may click (tap) on the ads

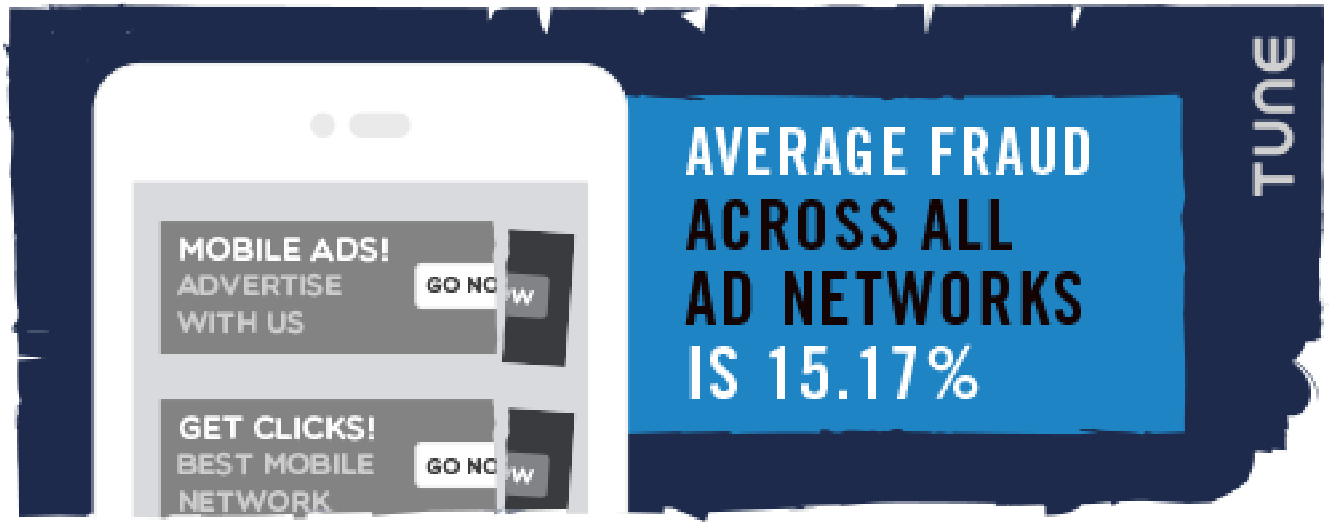
To protect marketers, an effective fraud prevention solution needs to address each one of the different fraud vectors.

WHAT THE DATA SHOWS: 24 BILLION CLICKS VIA 700 AD NETWORKS

TUNE uses dozens of measures to identify mobile ad fraud, including timing, geography, location, volume, device fingerprints, and more. Our fraud analysis reporting then highlights suspicious activity so you can verify results and compare ad networks against each other at a deeper and more comprehensive level than any other solution on the market

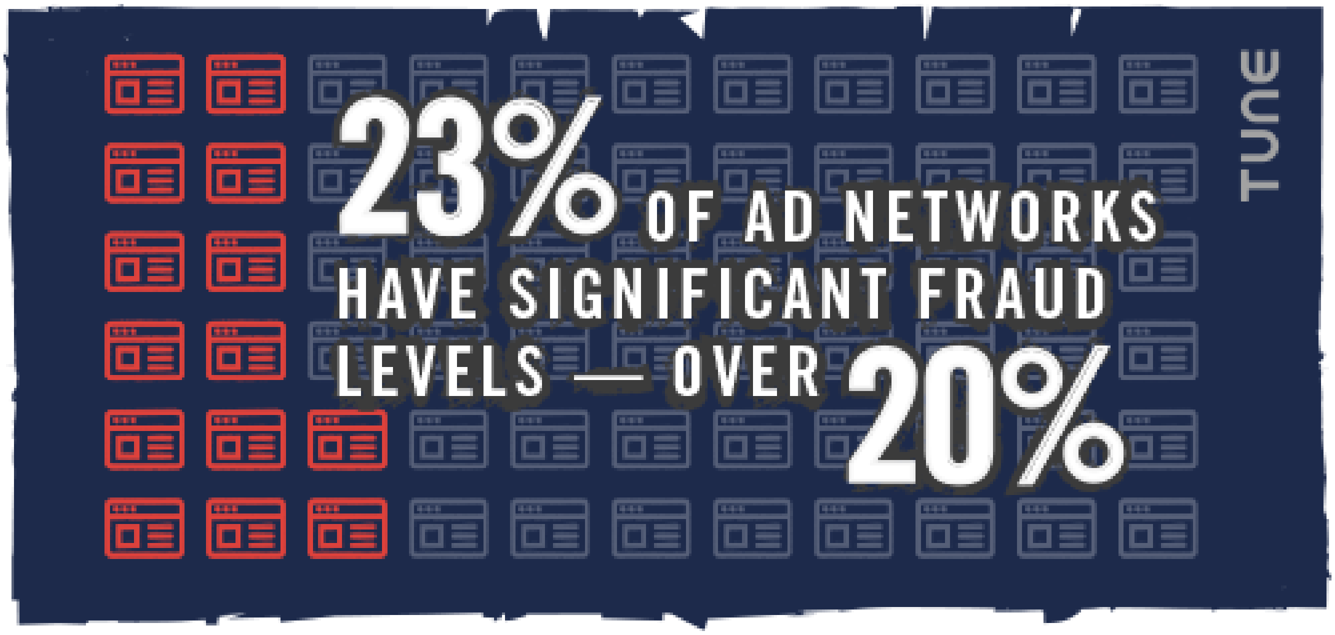
(Alternatively, marketers can "set and forget" fraud prevention tools to automatically cut off traffic that is clearly almost all fraud.)

What we've seen so far is concerning: **Average fraud across all ad networks is 15.17%.**



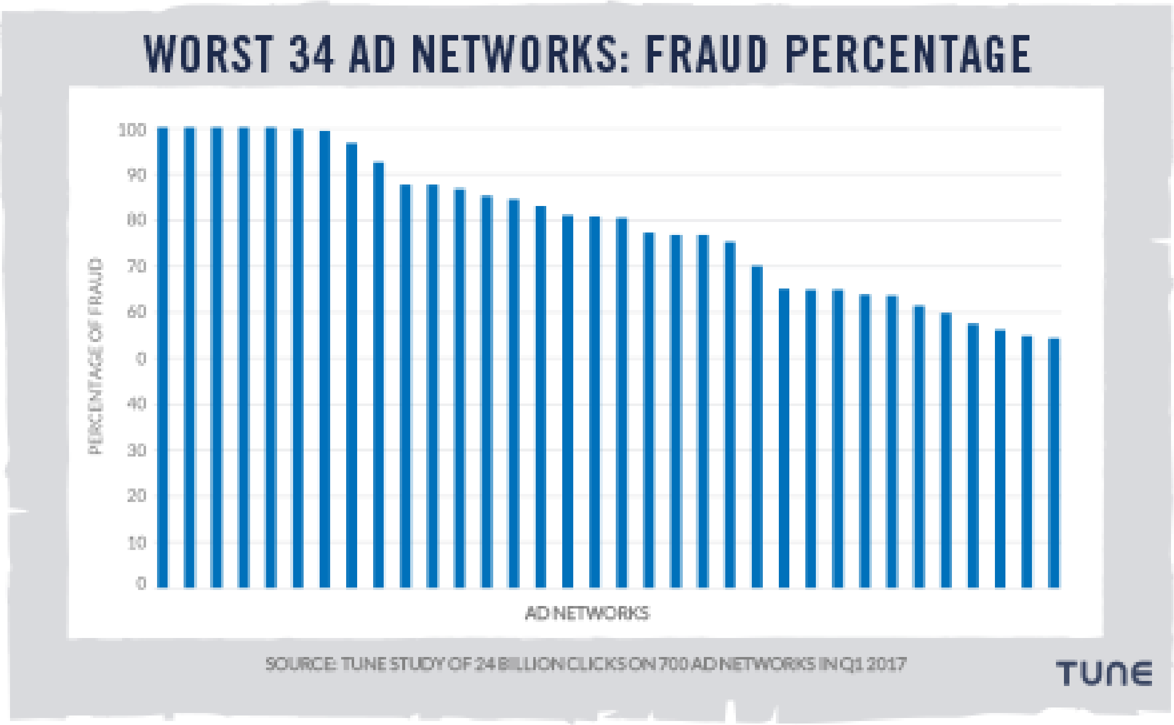
In addition, **23.3% of ad networks have significant fraud levels — over 20%.**

Some of these are plainly and simply bad actors who are enabling fraud, shortchanging marketers, and causing problems for the entire industry. Some of them are well-meaning companies that have paid far too little attention to the sub-publishers where marketers' ads actually run (more on that later).



It must be said that many ad networks have very low percentages of fraud, including plenty at 2% or lower, and a large number at under 5%. In fact, half of the 500+ ad networks that have significant traction and traffic have less than 5% fraud.

The problem is the higher percentages in the worst ad networks that bring up the all-networks average. If you look at the traffic patterns of the worst 34, here are the fraud percentages:



WORST 34 AD NETWORKS: FRAUD PERCENTAGE

SOURCE: TUNE STUDY OF 24 BILLION CLICKS ON 700 AD NETWORKS IN Q1 2017

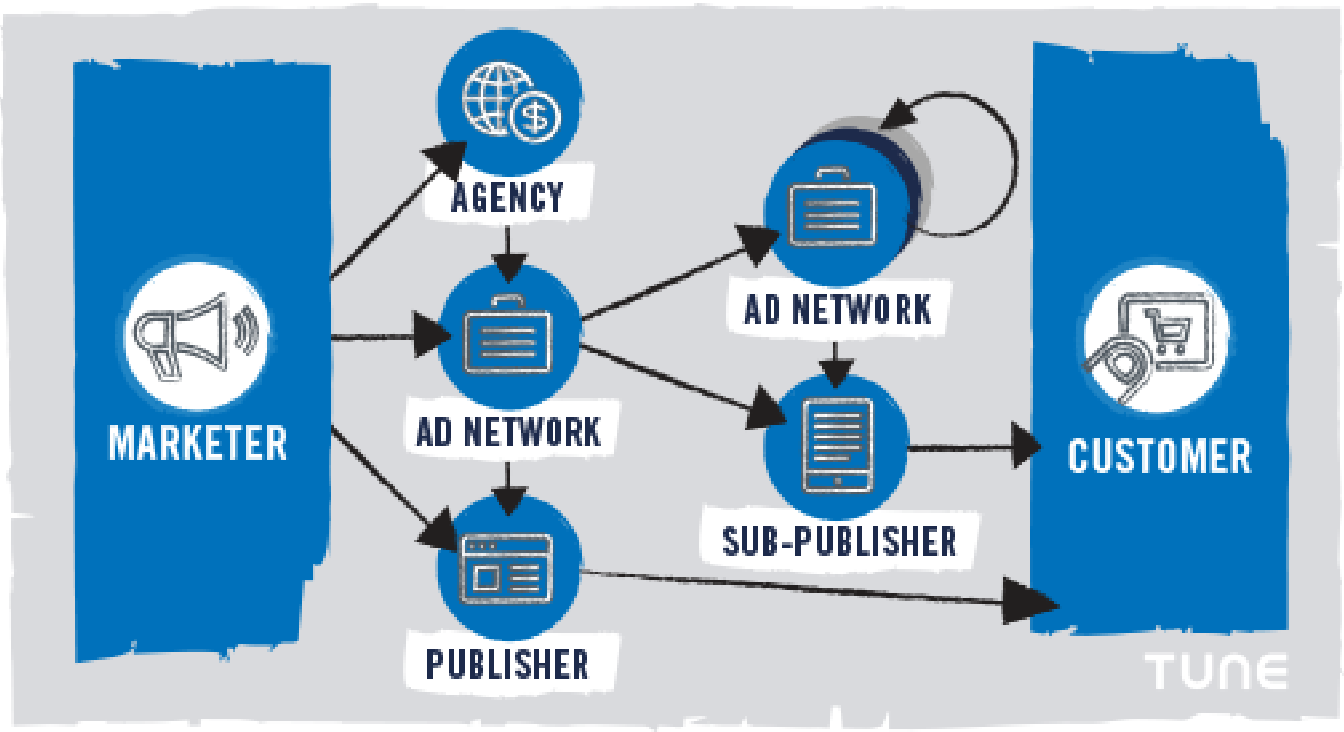
Clearly, there are some significant issues out there, and marketers who make the wrong choices can pay for it by sending their hard-earned marketing dollars straight into the hands of fraudsters. This reduces ROI and ROAS, of course, but it also funds exactly the kind of scammers that the industry needs to starve.

The unfortunate result: enabling even more fraud.

ARE AD NETWORKS ALL CROOKED?

In a word, no. The problem is largely a function of how ad networks work with each other, and with publishers.

Two things create cracks for fraudsters to find and exploit: **sub-publishers and re-brokering.**



"Often, ad networks re-broker ad traffic to other ad networks or to sub-publishers," says TUNE enterprise data evangelist Jim Tommaney. "One ad network is contractually working with other ad networks. This is generally legitimate as networks provide media buying, but questionable or fraudulent traffic can more easily enter the picture."

Breaking that down, here's what actually happens.

An ad network contracts with marketers to place ads in front of a desired audience of prospects and/or customers. The network places the ads with publishers that it has direct relationships with, but cannot itself fulfill the entire ad campaign. Marketers' demand (desire to place ads) exceeds the ad network's owned supply (available space for ads). So the ad network brokers with other networks who have access to supply (sub-publishers) in order to fulfill the demand.

In some cases, the re-brokering happens more than once. And in the re-brokering process, often to sub-publishers, traffic quality can suffer.

For example, marketers' original preferences for audience quality and location might not make it through to all of the sub-publishers' traffic. Top-quality ad networks work hard to ensure that any re-brokered supply meets or exceeds their partners' requirements, but some are not as diligent.

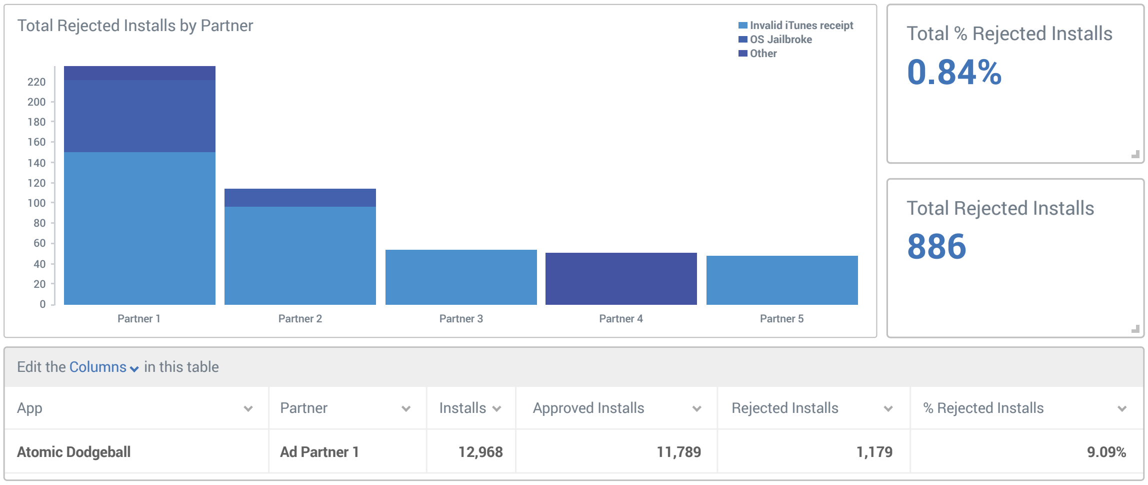
The end result in some cases is poor quality clicks, app installs, or views. In others, straight up fraud.

The reality is, however, that in all the complexities of re-brokering — which is often automated and at high speed — it is no longer easy for ad networks to know exactly, in real time, whether or not they are filling demand with legitimate, contractually-appropriate supply. In this fractured system, fraudulent publishers find cracks via which they can insert themselves into the legitimate ad ecosystem.

(And, perhaps not shockingly, the shadiest sub-publishers mislabel or misrepresent crucial characteristics of their supply, misleading higher-level ad networks.)

For this precise reason, marketers — and ad networks themselves — need tools that see all the way down to the base-level sources of traffic and/or attention that they paying for. That is exactly the tool that TUNE has built, and that TUNE is delivering for marketers: full visibility down the chain of ad networks and sub-publishers.

No other attribution company offers the same level of visibility down to the publisher.



Total % Rejected Installs

0.84%

Total Rejected Installs

886

Edit the Columns in this table

App	Partner	Installs	Approved Installs	Rejected Installs	% Rejected Installs
Atomic Dodgeball	**Ad Partner 1**	**12,968**	**11,789**	**1,179**	**9.09%**

"It is crucial to drill down to the sub-publisher level to isolate specific traffic sources for further analysis," says Tommaney. "This enables marketers to pinpoint where the fraudulent activity is coming from, and work with the ad partner to eliminate it."

This system-level complexity is precisely why fraud still exists today … in spite of innumerable attempts by many players at all levels of the adtech ecosystem to stamp it out. Most, if not all, fraud elimination efforts today treat ad networks as single, holistic units. With these first-generation fraud tools, if the ad network contains poor quality or fraudulent traffic, the only possible solution for marketers is to kill that ad network.

That seems like justice, and may feel like the appropriate thing to do. But it has two major problems.

First problem: Fraudulent publishers are resilient cockroaches

When stamped out in one network, the underlying fraudulent publishers simply shift focus to other networks. In other words, they tend to survive the attack — even if the ad network did not — and continue pushing their scammy payloads via other avenues.

“Historical methods to identify and eliminate fraud don't work in today's steroid era of fraud,” says Tommaney. “Naive recommendations to exclude outliers are like the tip of the iceberg … but the real fraud is underneath. The right response is to identify and eliminate bad actors via detection methods that are both transparent and extensible and focused on eliminating the bad traffic in its entirety.”

Second problem: Marketers could be cutting off their noses to spite their faces

It is not an exaggeration to say that even the largest and most significant ad partners on the planet — think hundreds of billions of dollars of market capitalization — have some degree of fraud in their networks. And yet, they may at the same time also provide great ROI for advertisers.

What’s happening?

They are good partners, and marketers are seeing significant return on ad spend from the 90-98% of the impressions, clicks, and/or app installs that are not fraudulent, in spite of the fact that some unscrupulous publishers have managed to worm their way into the ad network’s inventory.

“That, in fact, is the core difference in TUNE’s anti-fraud technology compared to every other solution on the market,” says TUNE chief executive officer Peter Hamilton. “TUNE’s fraud analysis reporting in the TUNE Marketing Console is currently the only system in the world that goes below the surface, seeing all the sources of traffic, clicks, and installs that build into a single ad network’s efforts — plus we have so many more developments coming soon.”

This is critically important, because having the ability to identify the unique components of your ad traffic that are fraudulent actually helps solve the problem, instead of just treating the obvious symptoms.

On the one hand, it spotlights the specific origin of fraudulent supply for everyone to see, which means that fraud can be stamped out at its source, and not scurry under a neighboring rock. This helps all marketers, including the initially-affected marketer … who otherwise could have the exact same source of fraud pop up in the very next ad partner he or she works with.

On the other hand, it also enables marketers to keep ad partners who, in spite of making a poor decision or being victimized by a sub-publisher, are actually delivering good or even excellent ROI.

In other words: Babies don't get tossed out with the fraud water.

"No one has actually tried to help both sides figure it out," says Peter Hamilton, TUNE's CEO. "It is clearly the responsibility for ad networks to supply high-quality traffic, legitimate views, and real-user app installs. Just as clearly, it's the marketer's responsibility to care, to measure, and to verify."

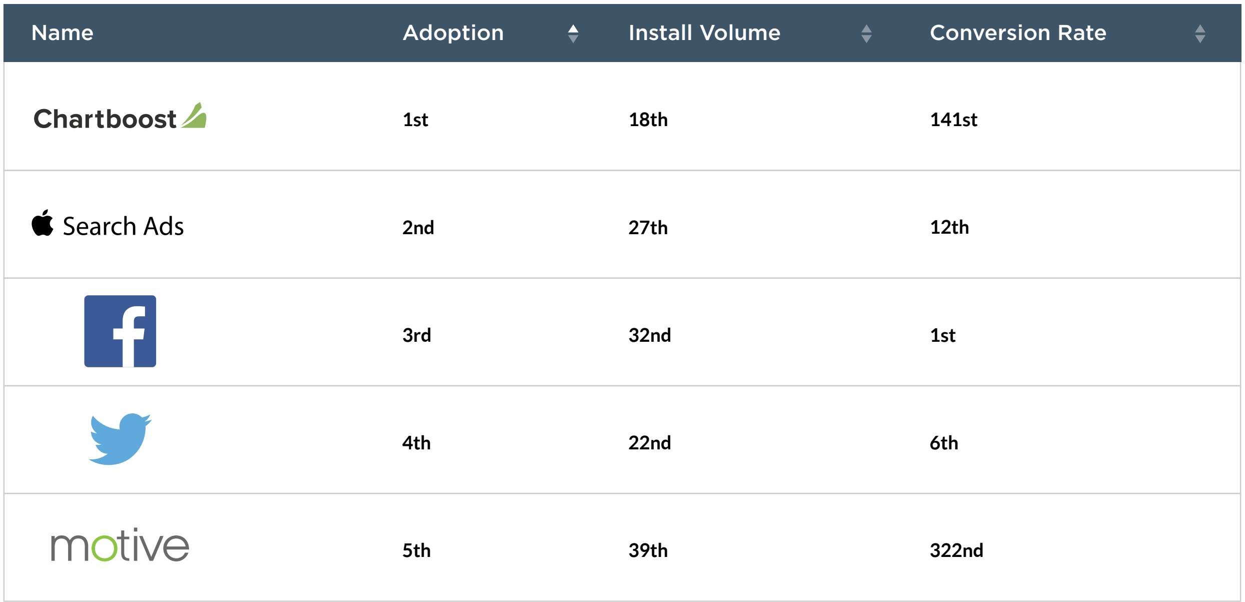
HOW TO FIND GREAT AD NETWORKS: START HERE

So how do you identify the right ad networks, who are taking the trouble to vet their publisher sources, and find the highest-quality ad partners to work with?

If you are just getting started, try TUNE's Mobile Advertising Index .

The Mobile Advertising Index is a partial public-facing view into what TUNE Marketing Console clients use daily to find the best ad partners: a window into the collective results of everyone using the platform. (Partners include brands such as Sephora, Sony, and eBay, and mobile-first publishers like Supercell, LINE, and Kabam. See more here.)

Select criteria for the kinds of ads you want to run, on which platforms, and in which geographies, and you'll be able to see what's working well. And, you can sort by the factors that matter most for you.



Name	Adoption ▲▼	Install Volume ▲▼	Conversion Rate ▲▼
Chartboost	1st	18th	141st
Search Ads	2nd	27th	12th
f	3rd	32nd	1st
🐦	4th	22nd	6th
motive	5th	39th	322nd

But beyond that, of course, TUNE's fraud analysis reporting is constantly operating to help you ensure that no matter what ad partners you pick, you can get protection from fraudulent behavior.

Your goal is that every dollar you spend on advertising drives business value. Our job is to ensure that happens.

One other very important tool marketers should be aware of: **Multiverse .** (It's free.)

With many different ad networks and marketing channels, it's challenging to understand your overall return on ad spend. Typical busy marketers might have five to 10 dashboards from various partners such as Google, Facebook, and multiple ad networks, plus perhaps spreadsheets or full low-level data dumps of performance, none of which are guaranteed to measure the same metrics in the same way.

The result is Excel hell: hours and hours of matching and normalizing data. Or, Multiverse, which does it all for you — for free — and lines up your attribution data with your ad spend data, side by side.

AD NETWORKS: WHAT YOU NEED TO DO TO SOLVE AD FRAUD

As we've seen, marketers need modern tools to verify that they are getting what they paid for, deep-diving diagnostics to understand problems that the tools identify, and automated technology to remove fraud from their pipelines.

But marketers are not responsible for the problem, and cannot by themselves fix it. That is each ad network's responsibility.

And ultimately, fixing fraud is in ad networks' best interest. Ad networks' very existence depends on trust from marketers: lose that, and marketers stop investing. When they stop investing, ad networks starve. So the networks have a vested interest in stopping fraud. This is not only a long term existential issue; it's a daily business success issue. After all, when marketers learn that they've been cheated, they often claw back tens or hundreds of thousands of dollars. Ad networks have little choice but to refund or replace the fraudulent ad deliveries.

Sometimes the conflicts even run into the millions of dollars.

But, as we've mentioned before, a big part of the problem is that in all the complexity, sometimes ad networks don't know exactly where and how fraud is entering their systems. Or it simply takes too long to get the right data and make it actionable.

"There's a core problem in the industry: time to information," says TUNE enterprise data evangelist Jim Tommaney . "Doing the analysis to find the fraud patterns can take 45 days ... and that can be tens of millions of dollars later. Now you're in a high-risk, high-volume, high-dollar, contentious relationship. TUNE's goal is to move the analysis all the way upstream, find the fraud immediately, and act immediately. In other words: measure faster, learn faster, and modify faster. Each additional feature you will see us release in the coming months further supports that real-time impact."

TUNE runs fraud analysis data daily, helping ad networks understand — and correct — their exposure in almost real time.

MARKETERS: WHAT YOU SHOULD DO IF YOU IDENTIFY FRAUD

Marketers are not without their own responsibilities.

Clearly, when they pay for a service, marketers have a legitimate right to expect to get what they paid for. Just as clearly, it is critical for buyers to periodically validate that they are getting what they were sold.

Marketers that care, and marketers that measure, are the ones we see succeed.

The first and most important line of defence is simple: Are you seeing ROI from your ad spend? In other words, are you making sales, are mobile users you've acquired using the app, are people downloading the white paper you advertised, and is your customer lifetime value looking good in comparison with customer acquisition costs?

In short, are there measurable activities happening post-ad that you can assign value to and determine ROAS, and show an overall positive pattern?

If so, you know something good is happening.

Even if so — and especially if not the case — marketers should regularly check their ad partners for compliance and quality. The TUNE Marketing Console offers precisely that capability, right down to the sub-publishers, and TUNE support personnel can help marketers understand what they're seeing.

If you spot fraud, there are two actions to take.

"First, act quickly. Cut off that source of traffic — this will save you from having to do clawbacks," says TUNE CEO Peter Hamilton. "Second, have a conversation with your ad partner ... review your insertion orders, and have a data-driven conversation based on the data you're seeing in the TUNE Marketing Console. Remember, you should be backing all of this out to incremental ROI. If you're not seeing the lift, the value should be obvious."

If the ad network is actually doing well on the whole, marketers can decide to simply request that they turn the fraudulent sub-publisher off. If the ad network is not doing well, marketers can exercise the nuclear option and terminate the relationship.

FIXING OUR INDUSTRY

Ultimately, marketers and ad partners need to work together to fix ad fraud. The past few years of failing to eliminate ad fraud via single-point, limited-visibility, first-generation fraud solutions is proof of that.

This conversation happens best in an open, data-driven discussion.

TUNE's new fraud analysis tools enable that discussion, and form the foundation for both marketers who can trust but verify what their ad partners deliver, and ad networks who can wash their own dirty laundry essentially in real time.

The result is cutting off the oxygen supply for fraudsters and illegitimate publishers.

And the result is more money for marketers to focus on their core mission: attracting new customers.