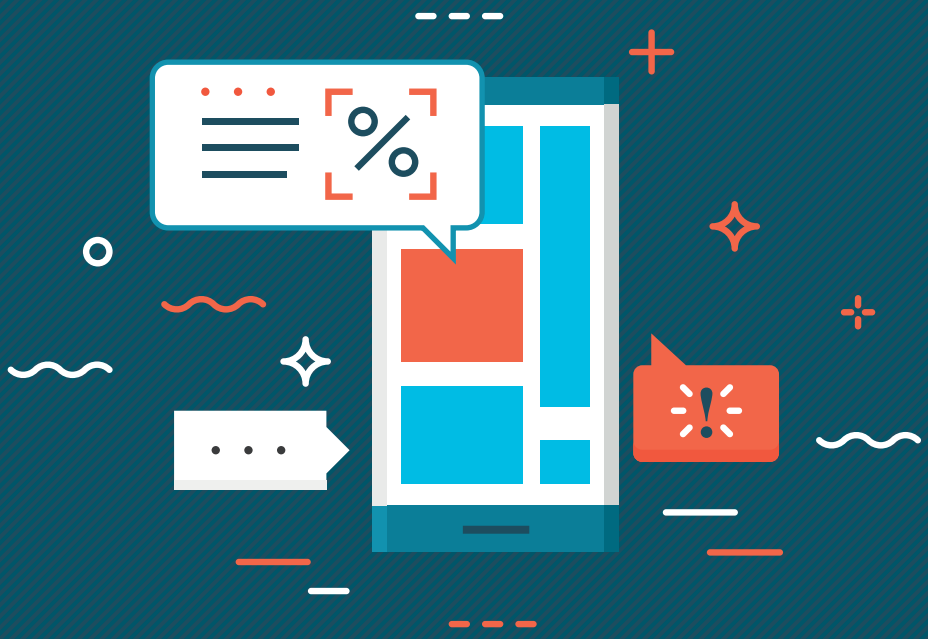
admonsters

PLAYBOOK

Mobile App Ad Quality



Sponsored by: geoedge Add Integrity

1 INTRODUCTION

While many mobile app publishers have struggled with monetization over the years, there are strong signs that the tide is turning and the mobile app channel has a lucrative future. However, the mobile ecosystem is chock full of bad actors looking to take advantage of legitimate publishers, advertisers, and users. As the last touchpoint before the user, the mobile app publisher has an enormous responsibility to thwart malevolent intent.

This playbook will dive into why the mobile app space is due for an uptick, and why bad actors and malvetisers are likely to become even more of a threat. We'll examine why your ad quality solution should integrate an SDK as well as key aspects to that toolkit and integration. Finally, we'll lay out best practices when it comes to working with ad quality providers and monetization partners.

WHAT'S A PLAYBOOK?

A playbook is an extension of what the AdMonsters community has been doing at our conferences for 20 years. A playbook solidifies what has made our events "must attend" for many digital strategists. By bringing people together to share learnings and best practices in a focused way, people can create a plan and avoid hours—if not days—of doing research on their own.

The AdMonsters playbook concept takes existing AdMonsters content (from conferences and AdMonsters.com) and, with the help of the AdMonsters community, "crowd sources" a document that outlines best practices on a particular topic. Our belief is that this will allow for a free exchange of ideas with the benefit of curation for accuracy. This document does not get into specifics around individual solution providers intentionally.

Great effort has gone into writing the playbook in a fashion that applies to as many publishers as possible without becoming too general. In a technology-driven industry like digital advertising, information quickly becomes obsolete. The intention is that, based on the feedback of the AdMonsters community, the next playbook will start to take shape and, with additional contributors, grow in both depth and breadth.

2 WHY IS THE MOBILE APP SPACE CHANGING?

Report after report shows that users are increasingly connecting and consuming content on mobile devices, with some even forgoing desktop experiences entirely. Brands know they need to engage their consumers on "the most personal of devices," but the creative options and targeting available has long been lacking.

This is still a young space—consider that Apple introduced the first iPhone in 2007, and then launched the App Store in 2008, truly heralding the modern app era. Mobile consuming habits have changed rapidly over the last dozen years, and continue to fluctuate. Though it's long been reported that consumers spend the majority of their mobile time within a few major apps, that trend is changing in the face of disenchantment with these apps and an increasingly diverse set of mobile users.

On mobile, the app environment is an optimal spot, data-rich environments that allow for immersive units that can theoretically grab a user's undivided attention. But the app space has been marred by slow technological development due to a perceived lack of revenue upside, the labor involved in building channel-specific technologies, and the dominance of players like Google, MoPub (Twitter), and InMobi.

Those factors have made many app publishers lean heavily on ad networks for fill. The black-box nature of ad networks is not good for publishers or advertisers alike, but many factors are aligning to inflate programmatic demand for mobile app inventory—see sidebar.

While ad networks certainly may fall prey (or in some cases even facilitate) malvertising and other unsavory acts, the vastness of programmatic channels truly open the floodgates for bad actors in an environment where the lack of transparency makes it easy to hide.

REASONS MOBILE APP INVENTORY IS GROWING MORE ATTRACTIVE

A prime way for advertisers to hypertarget users on mobile was through the mobile web. But the majority of US mobile web traffic comes through the Safari browser, and Apple has updated Safari's Intelligent Tracking Protection to disable third-party cookies and limit the effectiveness of first-party cookies. This means measurement and targeting on mobile web are limited if available at all. In addition to a device's advertising ID, apps often feature logins (which can be tied to other devices), cross-device targeting and measurement. The data-rich environments are quite attractive to advertisers—especially when the mobile web is virtually lights out.

- **Increasing interest in location data** for targeting purposes—data can be easily consented to connect via app.
- **An influx of location data** that can be conveniently leveraged in the mobile app space. The number of devices giving off location signals will only grow with the rollout of 5G networks that enable countless connections at high speeds.
- **The ability for app publishers to bypass SDK integrations** establishing deeper data relationships with demand sources.
- **In-app "header bidding"** is bringing mobile app publishers a greater variety of demand, through the programmatic pipes.
- **Major improvements in mobile creative** over static and sticky banners, including native experiences, more engaging units, rewarded video, and augmented reality.

3 THE DARK WORLD

The Wild West cliche gets thrown around a lot in digital advertising, but the lack of transparency in the mobile app environment truly makes it untamed terrain. Many ad-tech SDKs are virtual black boxes, and tag-scanning (or blocking) software that's popular on the web is ineffective.

Far and wide, publishers in the mobile app space recognize auto-redirects as their biggest malvertising challenge. Who hasn't been served a redirect on their mobile device in the past few years? They have turned into outright plague, but they also come in a variety of forms—from pop-up windows offering gift cards to kidnapping users to app stores to actually downloading apps and other software.

Real-time creative blocking has had a real effect on web redirects, where most transactions are tag-based easier to scan or block in real time. But tags don't exist in the mobile app space, and many SDKs are opaque, meaning it's hard to monitor let alone block bad creative before it lands in the app. Getting monitoring access at the very least within the app environment requires an ad-quality provider to integrate a software development kit (SDK).

LOW CPMS ARE WHERE MALVERTISING THRIVES.

While sources reported that higher-CPM demand from the United States and the European Union tends to be of good quality, there is a giant dropoff in CPMs for demand in other regions—and a giant uptick in malvertising. In addition to a real-time creative blocking solution. Considering dropping certain geos with low CPMs as well as carefully monitoring the relationship between floor prices and bad creative. According to the GeoEdge security team, there is a direct link between malvertising and low floor prices.

HOW DOES IN-APP DISPLAY AD-SERVING WORK ANYWAY?

In serving display ads on the web, the browser serves as a "communication hub" between the various servers involved (potentially SSPs, DSPs, and buy-side ad servers), handling calling, fetching, and redirecting. Through constant callbacks to the browser, all parties can share user data—that is drop and write cookies.

But with no browsers or cookies in mobile apps, in-app ad calls are relayed from one server to another through SDKs and APIs. This cuts down on time and end-device processing power, but it does limit the amount of data flow.

For example, in an RTB situation, the ad server relays the call to an SSP which then communicates with exchanges and DSPs and then relates the winning bidder's information to the supply-side ad server, which then calls back to the user. From there the user calls to the winning bidder's ad server as well as the CDN. In the case of instream mobile video, the mobile video player would actually be calling the supply-side ad server.

It also highlights the need for an ad quality provider to have its own SDK within the app for direct access to these transactions.

4 SDKs

SDKs are both the answer to ad quality issues... and a problem in themselves.

Used for a variety of applications including monetization, analytics, and security, software development kit is the app's access point out to other connected tech. However, developers tend to limit the number of SDKs an app uses for a variety of reasons, many tied to user experience:

- Difficult integrations and incompatible code;
- Latency issues, usually tied to size.
- Crash potential;
- And headaches related to software updates. An operating system update will likely require an SDK update, while an SDK update may require a publisher to get a new version of an app approved in app stores.

Limiting the number of monetization SDKs integrated has been a common practice; many in-app demand sources have also built simpler APIs that can handle the job. Especially with monetization technology, a single SSP or exchange can open up to a wide realm of demand sources, precluding the need for numerous SDKs. However, if an app is only using one SSP to reach out to numerous marketplaces, determining the sources of bad creative can become even harder than it already is.

To get the access it needs to prevent and track malvertising, an ad quality provider needs to integrate an SDK; an API won't cut it. And because user experience is their primary concern, product is more willing to integrate an ad quality SDK—minimizing the impact of auto-redirects in particular sounds fantastic.

Still, monitoring transactions—and potentially blocking creative—in real-time is a demanding task with a high potential to cause latency or crashes. And the app environment is not like the web where installing an ad quality provider requires a snippet of code—integrating (and removing) an SDK not only takes time, but app updates and app store approvals.

You need to choose your mobile-app ad quality partner even more wisely than you select other SDK partners (see sidebar). And this means data sharing—

which goes two ways. It's imperative you give your potential ad quality provider as much detail on your monetization and app setup as possible before getting feedback about what they can specifically do for you. In turn, the provider should be able to tell you just how their technology will affect your overall stack—and product.

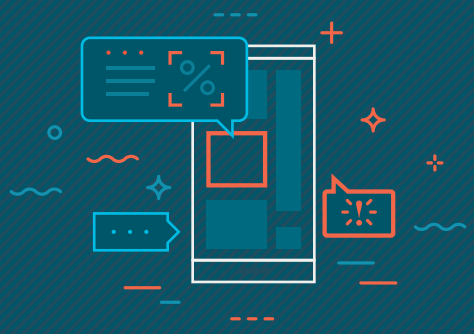
Then test, test, test. An SDK integration isn't forever, but because the process is resource-intensive, it's like an ad server migration—not something you want to go through very often (or at all). The whole update-and-app-store-approval process is particularly draining. Due diligence in the pre-integration and trial phases will pay off in the long run.

Finally, work in tandem with your ad quality provider, and deliver the feedback they need to improve the product—don't slack on the data-sharing! In-app ad quality is very much a work in progress, so the communication between you and your provider must be excellent. (As noted in the callout, 24/7 customer service is a must-have.)

Now is a great time to build a working relationship, because big changes are coming to mobile advertising—the rollout of 5G will vastly speed up connections, and probably open a slew of new doors for malevolent actors.

WHAT'S ACTUALLY IN AN SDK?

Don't mistake an SDK for an API (Application Programming Interface)—an SDK is a far more complex toolkit and may have numerous APIs, which are simpler interfaces between technologies. At the same time, SDKs can put a lot in a small package: tools (APIs), documentation, code samples, libraries, and processes are for developing applications for specific platforms, or bridging two platforms. A solid ad-quality SDK can be as small as 130 kb.



THINGS TO LOOK FOR IN SELECTING AN AD-QUALITY SDK

- **As much insight as possible** into how their technology works and their approach to identifying and catching unacceptable creative. A partner unwilling to get into the nitty gritty is a bad sign.
- **Support for both Apple iOS and Google Android.**
- **Support leading revenue generators such as interstitials and banner ads.**
- **Integrations with major mobile in-app ad players.** MoPub, AdMob, inMobi, Smaato, come to mind first.
- **Real-time creative blocking** has become table stakes for ad quality on the web, and should be for mobile apps as well.
- **Blocking capabilities according to app store policies.** iOS App Store and Google Play store have both strict guidelines regarding targeting different age groups. Make sure your provider blocks age-inappropriate ads.
- **Holistic solution to monitor all ad quality issues.** Real-time creative blocking is not the be-all, end-all of ad quality. Your provider must have extensive performance and latency monitoring tools.
- **Real-time blocking of pornographic and offensive ads.**
- **Revenue-driven decision making BI.** Your vendor should be able to provide you with all necessary data to approach and evaluate demand partners quality and performance.
- **Thorough customer support.** This is still-developing technology, so your provider better have live support to get you through rough spots. You guys should be in this together!
- **The latest schemes.** Scammers are always updating their tactics and strategies—some argue that they're always a step ahead of the blockers. Challenge your provider to be aware of the latest malvertising trends and how they're approaching new tactics.
- **A product roadmap.** Malvertisers might be constantly updating their strategies and throwing curveballs at ad quality providers, but that's no excuse for a lack of vision about innovating the product. While roadmaps are likely to change based on circumstances—and circumstances are ever-changing in ad-quality control—there should be a solid direction.

SDK VETTING

Some mobile-app service providers use the lack of transparency in the app realm to take advantage of the publishers they work with. Often this means an SDK that does more than advertised—and not in a good way.

An unsavory service provider may leverage its integration to clandestinely garner user location data, activate Bluetooth to receive and send information to beacons, and steal precious data in other ways. As mentioned in another callout, unsavory SDKs can be used to inject clicks that embezzle conversions or send false data on app downloads.

In an extremely sensitive data privacy moment, working with a duplicitous provider could actually amount to a regulatory violation. Vetting partners is critical in the mobile app space, and a rigid vendor certification process is something every app publisher needs.

This must go beyond ensuring the basics such as a valid headquarters address and tax identification number. Get written documentation of exactly what the vendor's technology is supposed to do, and then have your developers verify it as they putting the tech through the ringer. Be sure to note which data is going in and out—and out where. This can be particularly difficult with black-box SDKs—unwillingness to open up the hood and let some light into their workings is a bad sign.

Even after you've integrated an SDK, you need to keep monitoring to ensure tech changes don't catch you unawares. Don't set it and forget it!

HOW MANY SDKs ARE TOO MANY?

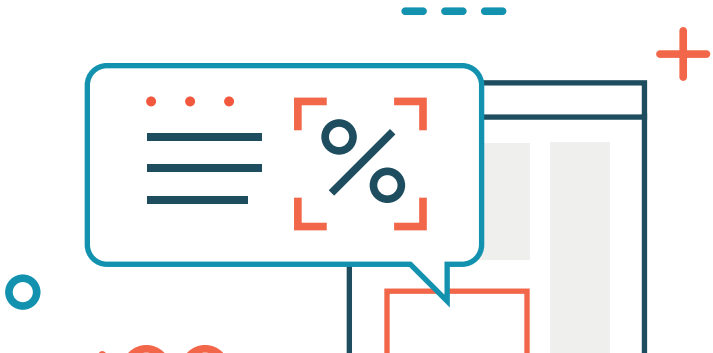
Depending on its function (and monetization strategy), a mobile app may have as few as four SDKs or something in the double digits. Reports on average number of SDKs from companies like AppFigure and SafeDK range from 6 to 18. There's no magic number for SDKs; in the past, product has tried to limit the number of integrations, but have become more lenient as SDKs have evolved to become lighter, less buggy, and overall more streamlined. Still, user experience concerns over latency and crashing will never go away, hence why vetting of service providers is so important.

OR YOU COULD BUILD YOUR OWN...

Many mobile app publishers are native to the environment and have been operating within its confines for a long time. They tend to hire specialists with great skills in building mobile technology and can develop tools internally for a variety of purposes, such as creative blocking. And as you know, technologies don't always play well together—building tech in-house often ensures the product functions well with your core tech (though not necessarily external technologies).

What you lose by building in-house is the expertise and experience of a third-party ad quality tech provider. These guys have been singularly focused tracking down and averting malvertising for years, and employ security investigators that are tracking down the latest schemes. Preventing malvertising is literally their business.

It's less about "Can I build it?" than "Do I have the experience and necessary resources to make it function well?" Keeping up with innovative scammers requires dedicated personnel. Do you want ad-quality ensurance to be a core competency?



5 BEYOND THE SDK

While integrating an ad-quality SDK is an essential step in minimizing malvertising within your app, it's really only the first one. Where are those bad ads coming from? No SSP seems to be immune, which is why monitoring and scanning are necessary functions beyond real-time creative blocking.

But these ad-quality tools are ultimately futile if you don't confront your demand partners about the bad ads coming through their pipes. As publishers cull their monetization partners, high-quality demand is a premium. SSPs and exchanges are increasingly focused on filtering out malvertising sources that are denting the overall quality of their ads.

So beyond integrating an ad-quality SDK, you need to establish a feedback loop with your demand partners to easily pass information on low-quality advertising and malvertising. The right ad-quality tech provider should be able to assist you in this.

We hope this playbook has shown you inside the mobile app arena, and why a mobile app advertising renaissance will also bring a new wave of bad actors. Only an SDK will enable an ad-quality provider the insight it needs to prevent malvertising. While app product has been wary of SDKs in the past, the need to mitigate auto-redirects in particular will

But not just any ad-quality provider will do. Revenue teams need to ensure the ad-quality SDK meets the same rigorous standards as all other SDKs, and that the provider is transparent with its tech and ultra-communicative.

The mobile device is the most personal of all devices, so user experience is always top of mind. The revenue team is tasked with balancing app monetization—which has been difficult—with safeguarding user experience—also difficult! It's not an easy job, but there's no group better to take it on.

GedEdge's mission is to protect the integrity of the digital advertising ecosystem and to preserve a quality experience for users. GeoEdge's advanced security solutions ensure high ad quality and verify that sites/apps offer a clean, safe and engaging user experience, so publishers and app developers can focus on their business success.

App Developers and publishers around the world relies on GeoEdge to stop malicious and low-quality ads from reaching their audience. GeoEdge allows publishers to maximize their ad revenue without quality concerns, protect their brand reputation and increase their user loyalty. GeoEdge guards digital businesses against unwanted, malicious, offensive and inappropriate ads – without sacrificing revenue.

To learn more, visit: www.geoedge.com

AdMonsters is the global leader in strategic insight on the future of digital media and advertising technology. Through our conferences, website, and original research, we offer unparalleled in-person experiences and unique, high-quality content focused on media operations, monetization, technology, strategy, platforms and trends. Founded in 1999, AdMonsters began serving the advertising operations professional through live media and its online community. We provided a forum to share best practices, explore new technology platforms and build relationships. Today's expanding ecosystem now includes publishers and content creators, agencies, SSPs, DMPs, DSPs, RTB and service providers, technology and platform developers, advertising networks, brands, and investors.

This vibrant community is forward-looking and results-oriented. Their success depends on strategic insights about technology and monetization, and the exchange of actionable peer-to-peer best practices. AdMonsters has built its reputation on providing objective editorial leadership based on deep, real-world expertise. We have continued to evolve our editorial strategy to address the changing needs of the market and, as a result, AdMonsters has attracted a highly focused audience who are at the forefront of the industry, and leading marketing partners have found AdMonsters to be a powerful channel to reach these decision makers. Today, our portfolio of integrated media solutions includes industry leading live events, our innovative Connect content solutions, email marketing programs, and more.

As of March 2015, AdMonsters is part of the Access Intelligence family of companies.

For more info:
See admonsters.com
Follow us on Twitter: @AdMonsters
Facebook: facebook.com/admonsters

Media contact:
marketing@admonsters.com
Sponsorship contact:
sales@admonsters.com

sponsored by: