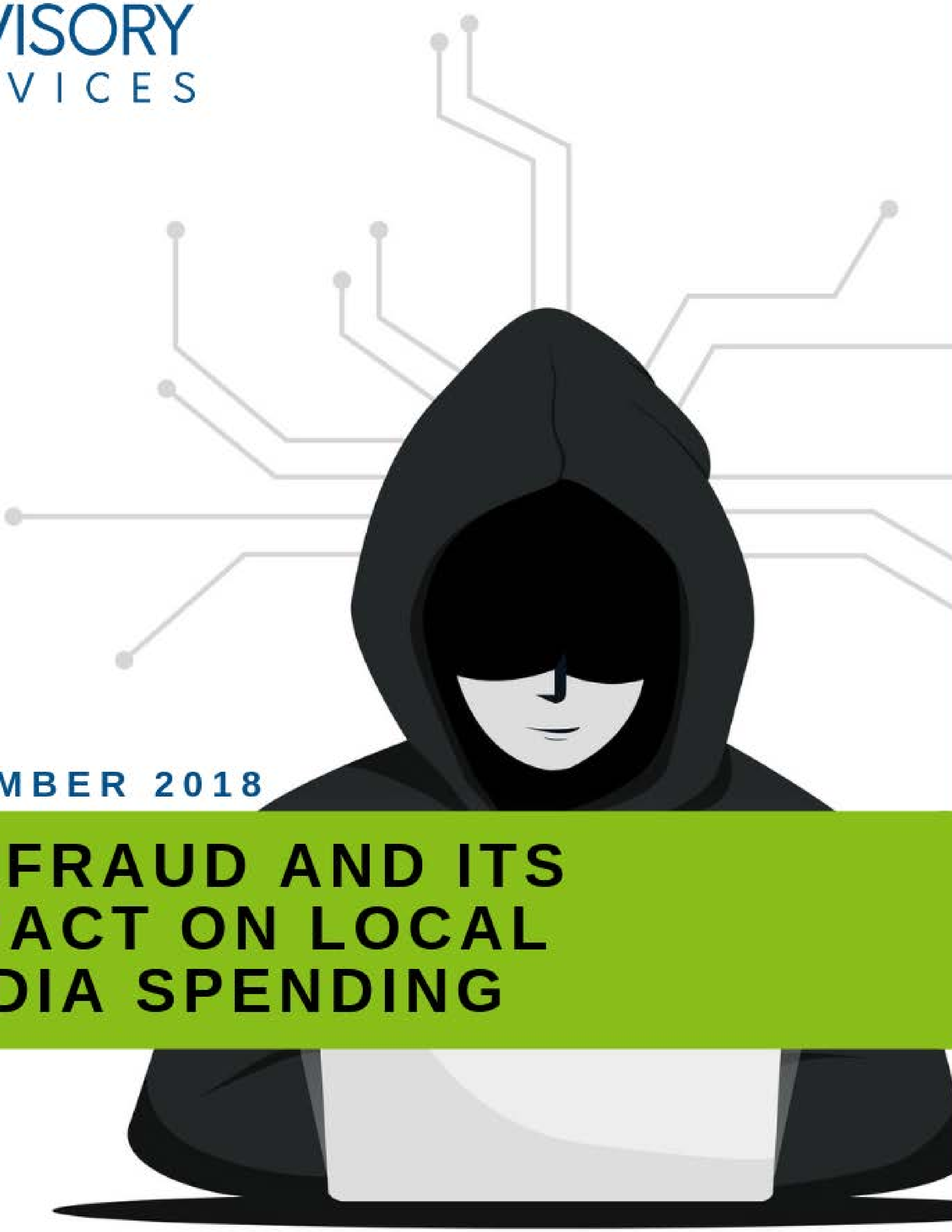
BIA ADVISORY SERVICES



DECEMBER 2018

AD FRAUD AND ITS IMPACT ON LOCAL MEDIA SPENDING

CONTENTS

FIGURES

EXECUTIVE SUMMARY

As a follow-up to BIA's September 2017 report entitled: "Ad Fraud in Targeting Local Audiences" we will present new data, learnings, and insights for marketers that target local audiences as well as publishers who have local audiences.

Ad budgets in local media continue to shift to digital. Marketers continue to increase their use of programmatic technologies. The confluence of these two trends have led marketers to spend more on geotargeted programmatic campaigns to reach local audiences. It may seem logical to target devices that are in a specific geolocation instead of buying media from local publishers, perhaps even cheaper. But what if those devices were not real mobile devices? Instead, they were fake mobile devices – made from mobile emulator software – that pretended to be in the desired geolocation.

As the saying goes, "you get what you pay for." The cheaper ad inventory is the result of ad fraud, where cyber criminals use fake mobile devices to load fraudulent ad impressions to rip off marketers. The mobile emulators are so advanced, they can download and install apps, launch and interact with those apps, and pass fake GPS locations and other sensor details.

Criminals create large numbers of mobile emulators at the same time in data centers. These fake mobile "devices" spoof their locations to create large fake audiences that appear to be in local markets that marketers want to target. The ad impressions are often less expensive, or even very cheap compared to ads sold by local publishers. This is extremely tempting for marketers; but they should be wary of their ads are being shown to software, not humans.

Fraud detection technologies are not able to catch this fraud because they do not work in mobile environments, particularly mobile apps. So even though they may report that fraud is low, is likely that they are simply not detecting it. So, if marketers placed their ads on local publishers' sites, which are visited by the people who live in those local markets, their ads are likely to be shown to real humans (in other words, properly targeted). The risk of exposure to ad fraud from fake mobile devices is much lower.

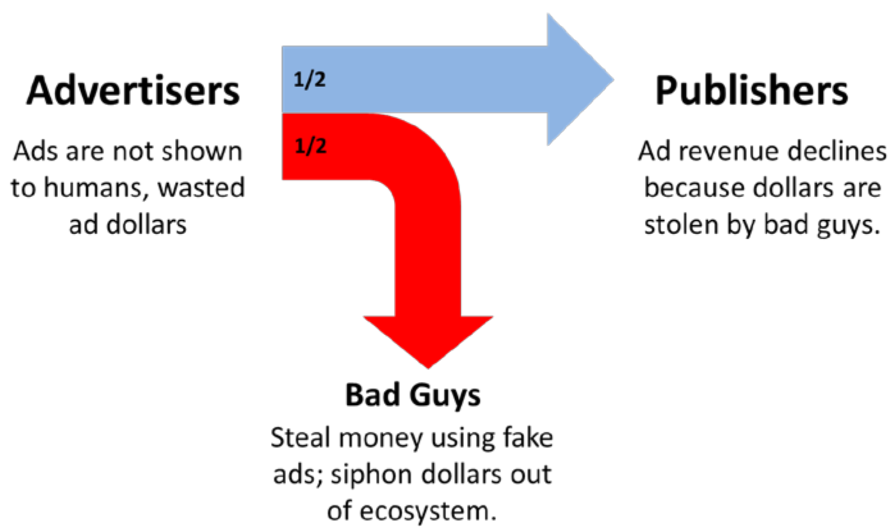
AD FRAUD REFRESHER

Digital ad fraud is fraud. Marketers pay for digital ads, expecting that their ads are shown to humans who visit websites and look at web pages. **Ad fraud is when the ads are not shown to humans, or not even shown at all.** Fraudsters use algorithms and other automated software to generate pageviews on websites or mobile apps in order to generate fake ad impressions.

This "inventory" of ad impressions is designed to steal ad dollars. These ads were never shown to a human. Criminals can also use malicious code to manipulate analytics to make it appear that millions of ad impressions were delivered, when actually no ads were even served; or they can trick analytics to make "rotten apples" (e.g., unviewable impressions) appear to be "fresh apples" (e.g., viewable impressions) so they can sell them for full price.

Criminals have been targeting large national marketing budgets for years. Now, as more dollars in local marketing budgets shift into digital, these budgets are attractive targets for ad fraud as well, and accessible through the same programmatic technologies used to commit fraud on the national level.

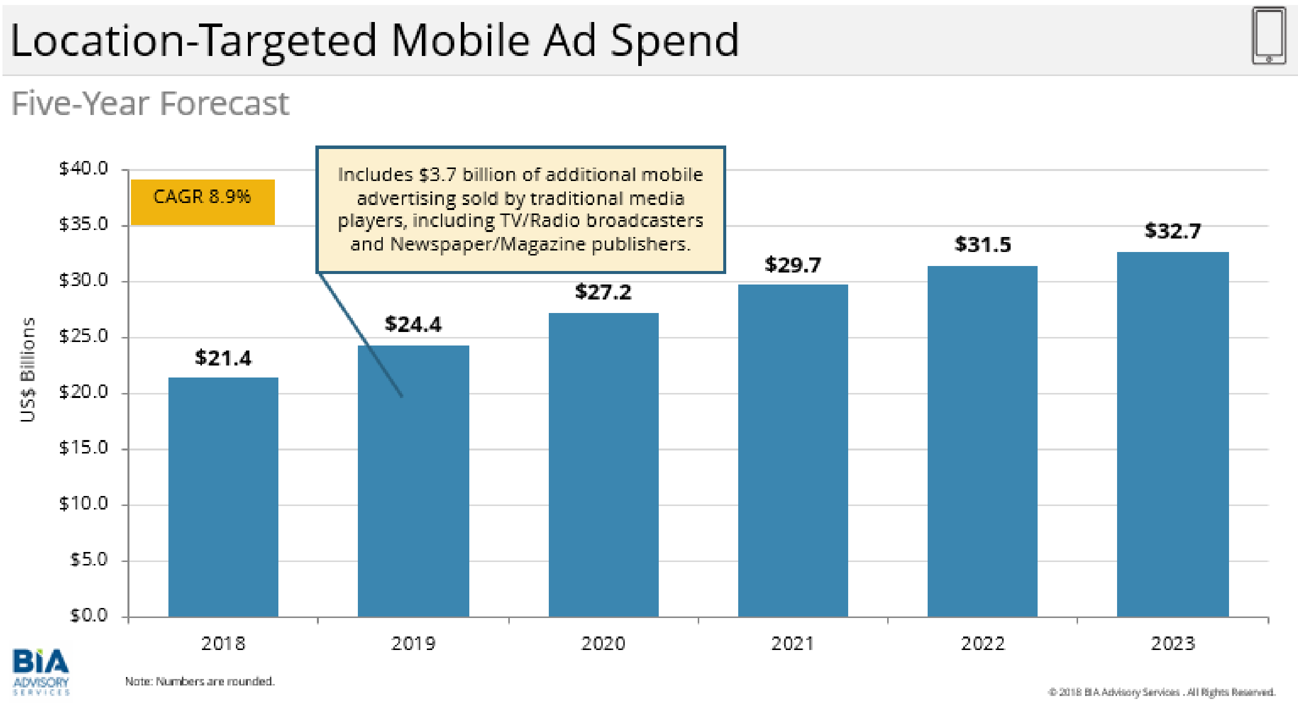
Figure 1. Why Is Ad Fraud Bad?



Source: BIA Advisory Services and Marketing Science Consulting Group, October 2018

As we show below, location-targeted ad spending just in mobile web and apps will increase significantly from 2018-2023 from $21.4 billion to $32.7 billion.

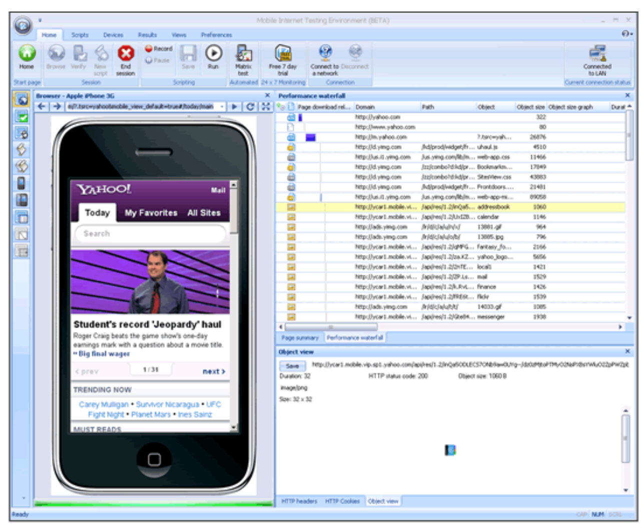
Figure 2. Location-Targeted Mobile Ad Spend 2017-2023



The bad guys are fake mobile devices –mobile emulator software – to create what appears to be local audiences. The emulator software creates fake GPS locations that appear to be in geolocations that marketers want to target.

This fake ad inventory is offered for sale in programmatic ad exchanges and marketers are tempted to buy these geotargeted ads because they are often less expensive than buying from real local publishers. But of course, these ads are not shown to humans, but instead created by automated software. The marketer is getting ripped off, even though the prices are cheaper.

Figure 3. Mobile Emulator Software



WHY ISN'T THIS CAUGHT BY FRAUD DETECTION TECHNOLOGY?

Fraud detection technologies were originally designed to look for bots – fake users that visited webpages to cause ads to load. So, while they can detect bots in desktop and laptop environments, those technologies don't work well in mobile, or don't work at all in mobile apps. They cannot detect any bots and therefore will miss detecting the fraud.

While there are SDKs (software development kits) that detect for fraud in mobile apps, the criminals are unlikely to add fraud detection into the apps they are using to deliberately commit fraud; just like bad guys don't put fraud detection analytics on sites they intend to use for fraud. There are many other limitations, too technical to delve into in this white paper, that make existing fraud detection technologies ineffective at rooting out fraud.

WHAT SHOULD MARKETERS TARGETING LOCAL AUDIENCES DO?

Marketers should always keep in mind the saying "you get what you pay for." This applies to digital advertising as well. **If you are targeting local audiences by buying geotargeted ads in programmatic exchanges and the CPMs are so low they appear to be too good to be true, they probably are.**

If you are aware of ad fraud, then you understand that creating fake inventory out of thin air using software costs them next to nothing; this is how they can create and sell such vast audiences that appear to be in the local markets you want to target. Fraud detection technologies are not able to catch this kind of fraud, so you should not be overly reliant on them.

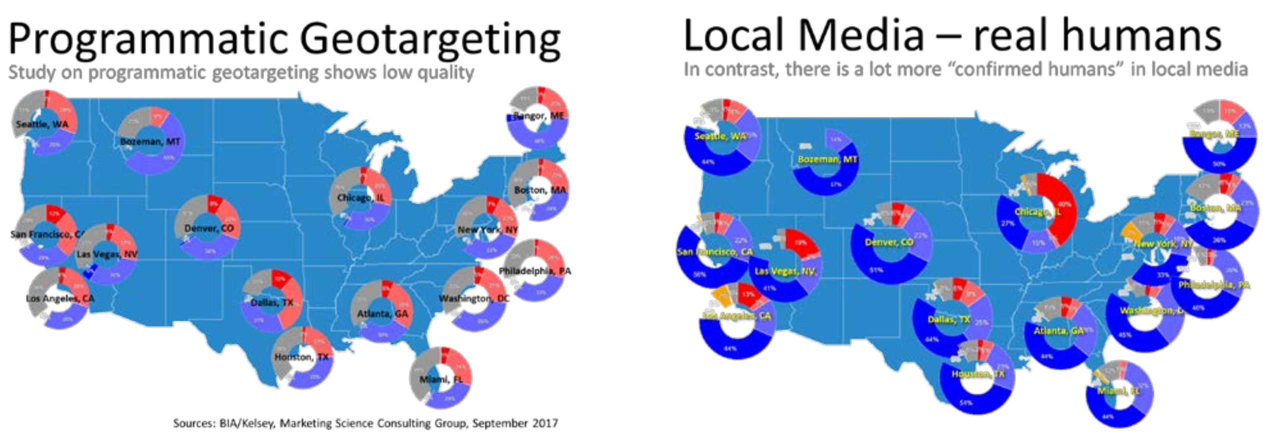
You should examine your own analytics to look for any signs of strangeness, for example – bounce rates that are too high, or too low; visitors that all use Android devices and no iPhones or iPads or desktop devices whatsoever; zero time-on-site visitors, etc. Even though fraud detection marked the traffic is valid, something is still wrong with it. It is likely that it is not human, so you are not getting what you paid for.

Marketers can also reduce their risk of exposure to ad fraud by buying from the local publishers that have local human audiences. Of course, the CPMs will be higher, but that's because humans visiting websites is a scarce commodity.

If you want to show your ads to humans, instead of to bots and mobile emulator software, then buying media from local publishers will still be worth it. The ultimate way to tell is by tracking your business outcomes.

There should be an obvious correlation between showing your ads to humans and higher ROI, compared to showing ads to bots and fake mobile devices.

Figure 4. Programmatic Geotargeting versus Local Media Audiences



WHAT SHOULD LOCAL PUBLISHERS DO?

Local publishers have real human audiences – the people who live in those DMAs and local markets. These publishers should avoid actions that increase their risk of ad fraud and decrease the value of their human audiences. The most important of these is to avoid the temptation to "buy traffic."

There is a finite number of humans that go to websites, the sites that have local content that appeal to only the residents who live there. Any vendor that purports to have large quantities of traffic may literally have just that – traffic. They never said it was human. It is just traffic that they can send to your website.

Where do you think that traffic comes from? Are there a whole bunch of humans with nothing to do but to go to websites they are told to visit, to generate said traffic? Of course not. So, the vendors are selling or re-selling bot traffic – automated software that repeatedly loads webpages. Even if the traffic appears to be "valid" according to current fraud detection tech companies, it still doesn't mean it is human.

Local publishers should also resist the temptation to sell "remnant" inventory in programmatic exchanges, hoping to get just a bit more ad revenue. Those assumptions may not materialize into any substantial new revenue. In fact, after the "ad tech tax" of 40 percent to 80 percent, the publisher is left with as little as 20 percent of the already-low CPM that their ads were sold for. On top of that, there is the following unintended consequence – some media buyers deliberately hold off on buying from the publisher so that inventory goes remnant, so they can buy it cheaper on the ad exchanges. The unintended effect is that the publisher has even more unsold inventory and they get even lower prices for their inventory.

Finally, local publishers should also educate marketers who buy from them about the dangers of ad fraud – i.e. buying lower cost, geotargeted ads on programmatic exchanges, thinking that they are targeting the same local audiences. They should be aware that those low-cost ads are being shown to fake mobile devices – software that is pretending to be in that geolocation.

ABOUT THE AUTHOR

AUGUSTINE FOU, PH.D.
Cybersecurity and Ad Fraud Researcher
Marketing Science Consulting Group

Dr. Augustine Fou is an industry-recognized thought leader in digital strategy and integrated marketing, and former Chief Digital Officer of Omnicom's Healthcare Consultancy Group, a $100 million agency group serving pharma, medical device, and healthcare clients. Dr. Fou has over 20 years of management consulting experience and hands-on experience in creating and optimizing marketing across traditional and digital channels. Dr. Fou teaches digital and integrated marketing at Rutgers University and NYU. Dr. Fou completed his PhD at MIT in Materials Science and Engineering at the age of 23. He started his career with McKinsey & Company and previously served as SVP, digital strategy lead, McCann/MRM Worldwide.

BIA ADVISORY SERVICES AD FRAUD SERIES EDITOR

RICK DUCEY
Managing Director
BIA Advisory Services

Rick Ducey is managing director, leading BIA's strategy consulting practice. Ducey also serves as practice lead and adviser to an affiliated investment banking firm, BIA Capital Strategies, Ducey is a sought-out expert for his coverage and analysis of how disruptive technologies, emerging competition, shifting consumer demographics and media usage trends drive changes in the media ecosystem.

Prior to BIA, Ducey was senior vice president of NAB's Research and Information Group. Ducey received his B.A. from the University of Massachusetts at Amherst, M.S. from Syracuse University, and Ph.D. from Michigan State University.

ABOUT BIA ADVISORY SERVICES

BIA is the leading research and advisory firm focused on the advertising and marketing marketplace. We deliver research, forecasts, analysis, competitive intelligence and market strategies produced by our team of analysts, strategists, economists, data scientists and digital and traditional media industry experts.

Our proven advisory services and consulting methods put our clients in the best possible position to compete and stand out in today's multiplatform, interactive world.

We are pleased to announce our Programmatic Program that features a series of papers and webinars that will help our clients understand the potential of programmatic.

We also publish an advertising intelligence platform, BIA ADVantage. Contact us today for more details: info@bia.com.

Connect with us:

www.bia.com

Local Media Watch blog

@BIAAdvisorySvcs

www.facebook.com/bia

BIA's daily newsletter

