BIA Kelsey

AD FRAUD IN TARGETING LOCAL AUDIENCES:

Programmatic Geotargeting vs. Local Direct Media Buys

October 2017

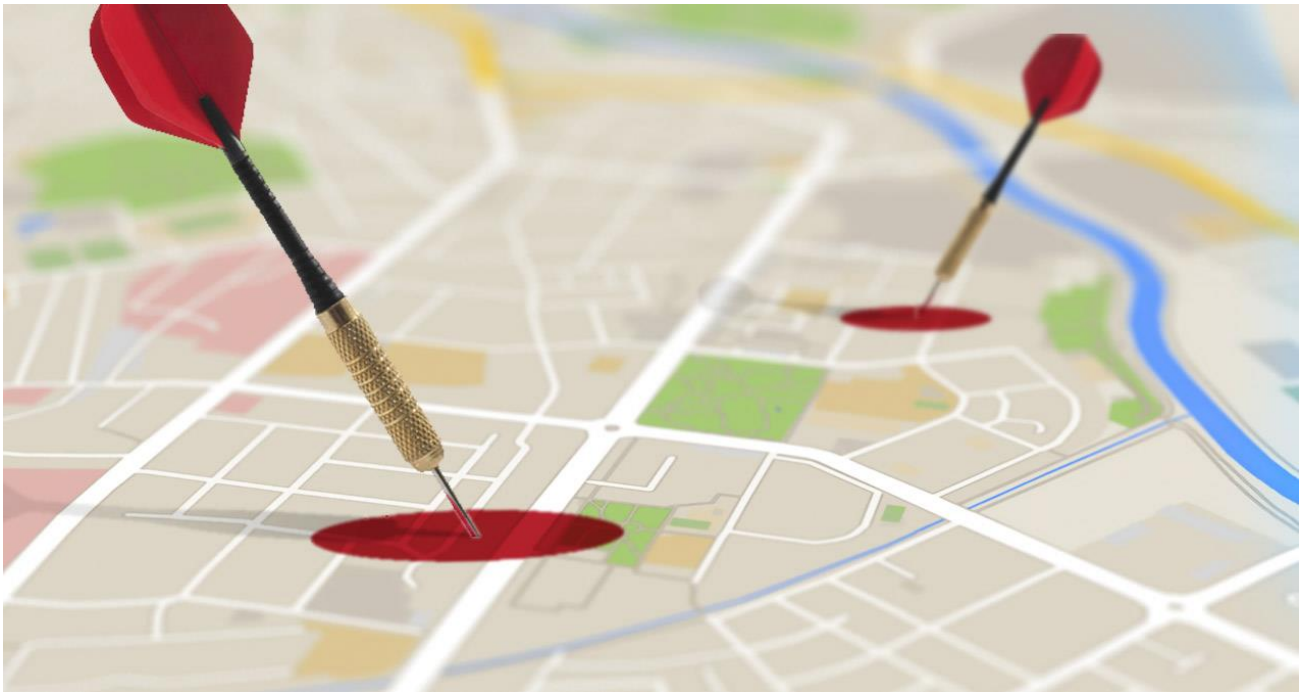
RICK DUCEY
BIA/Kelsey

AUGUSTINE FOU
Marketing Science Consulting Group

BRAD ADGATE
BIA/Kelsey

Contents

Figures



Executive Summary

BIA/Kelsey estimates that fraud in geotargeted programmatic media buying is a multibillion-dollar problem. The problem will get bigger as ad spend continues to shift into digital, and more specifically into media targeting local audiences. Fraudsters "go where the money is" and focus on "easier money." BIA/Kelsey forecasts that ad spending in local media will reach nearly $76 billion by 2021, making it an attractive and lucrative target for cybercriminals. Ad fraud is siphoning revenue away from legitimate publishers and delivering the wrong audiences to advertisers. Advertisers spending ad budgets to target local audiences and local media publishers alike should not only be aware of the risks of ad fraud but also take proactive action to contain this growing threat.

With respect to ad fraud, there are different levels of risk for marketers when using geotargeted programmatic media compared to direct media buys from local media outlets.

Geotargeting in programmatic media means targeting users based on approximations of their geolocation at any given time. This is done most often by estimating their location using the IP address rather than using real GPS location data. Because of this, the location is an extremely coarse, at best.

Buying media direct from local media outlets means putting ads on the websites of local radio, newspapers, and magazines. The audiences of these local media websites are typically the residents of the city, region, or DMA (Designated Market Area). This form of "targeting" does not rely on geolocations approximated from IP addresses.

The primary reason for the risk of fraud in geotargeted programmatic media buys is that fraudsters can make their bots appear to be coming from any geolocation through a variety of techniques including passing fake geodata or using proxy IP addresses that appear to be in certain geolocations. In this way, the advertisers using geotargeting in programmatic may be tricked into paying for ads shown to users that are not humans and that are pretending to be in the geographies targeted. The fraudsters' bots can also simulate pageviews, clicks, downloads, and other parameters typically used to assess audience engagement, thereby giving encouraging but false reports of campaign success.

BIA/Kelsey, in collaboration with Marketing Science Consulting Group, conducted a series of studies to assess the risk of fraud in programmatic media, targeting local audiences. The average rate of fraud across 16 DMAs was observed to be about 6%. Using this average, extrapolated to all DMAs with measured local ad spend, BIA/Kelsey estimates on an annual basis almost $3 billion is at risk of geotargeting ad fraud, using current estimates of the amount of local ad spend that is currently spent in digital and online media. This number is likely to continue upward as marketers continue to increase allocation to digital.

Preliminary recommendations from BIA/Kelsey include:

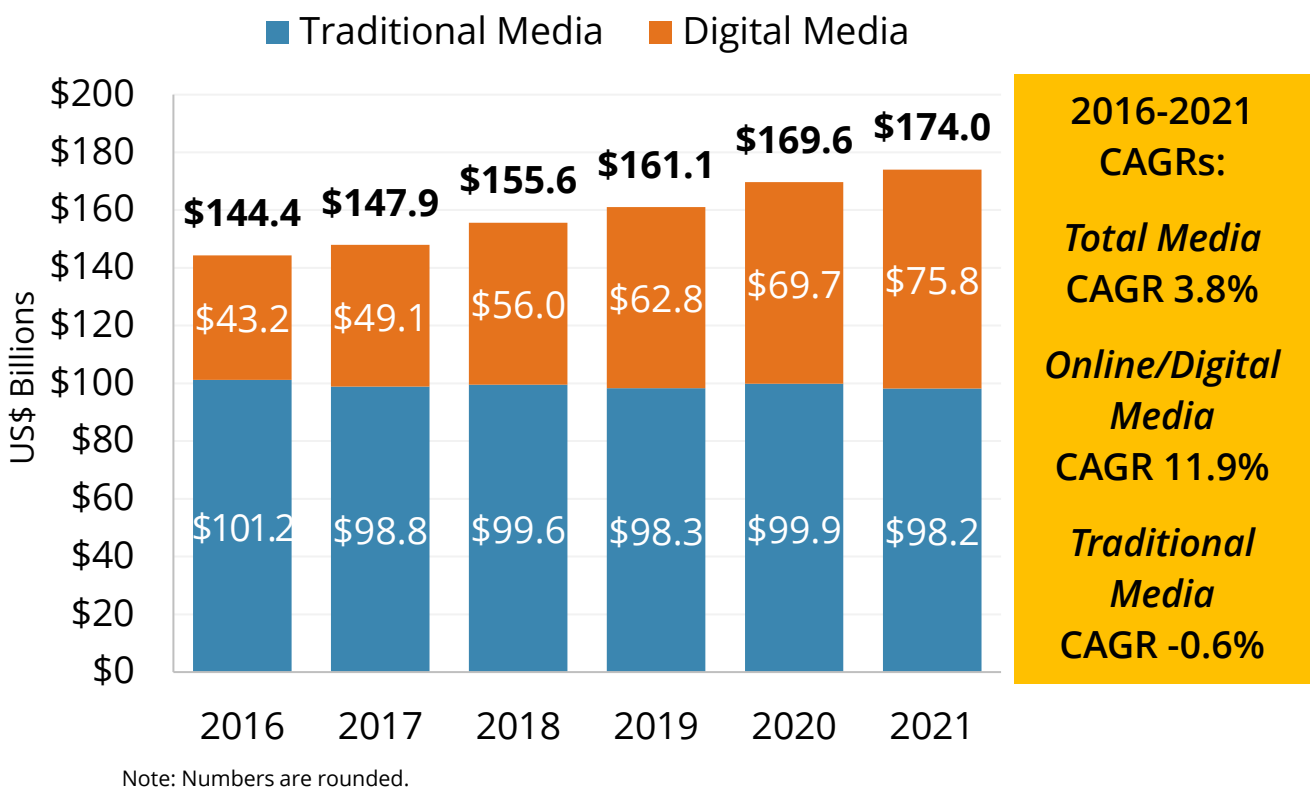
1. **Programmatic Geotargeting vs. Local Direct Media:** Buying geotargeting media through ad exchanges may not exhibit the same quality as buying direct from local media publishers.
2. **Ad Fraud Variance Across DMAs is Not Meaningful or Actionable:** While there was observed to be differences in the rate of fraud across the DMAs studied, the variations are not meaningful or actionable. For example, higher fraud in San Francisco or Dallas does not mean a marketer should spend less in those DMAs.
3. **Geotargeted Ad Fraud is a Scaled Problem:** Ad fraud in geotargeting campaigns can come from fake mobile devices which create fake geolocation data, in order to match the targeting of the campaigns, enabling them to steal ad dollars from local media ad spend.

Defining, Sizing the Ad Fraud Problem in Local

Marketers and agencies are investing more of their advertising dollars to target local audiences. BIA/Kelsey forecasts that national brands alone will increase their local media investments and activations by over $17 billion from 2015-2020. Unfortunately, wherever a lot of money changes hands, we tend to find less well-intentioned actors. With increased spend targeting local audiences, we will see increased ad fraud.

How effectively can we detect and protect against this type of ad fraud? BIA/Kelsey sizes this as a multiple billion-dollar problem. Ad fraud is siphoning revenue away from legitimate publishers and delivering the wrong audiences to advertisers. The problem will get bigger as more ad spend shifts into digital and specifically locally targeted media. BIA/Kelsey forecasts that digital ad spending targeting local audiences will reach nearly $76 billion by 2021.

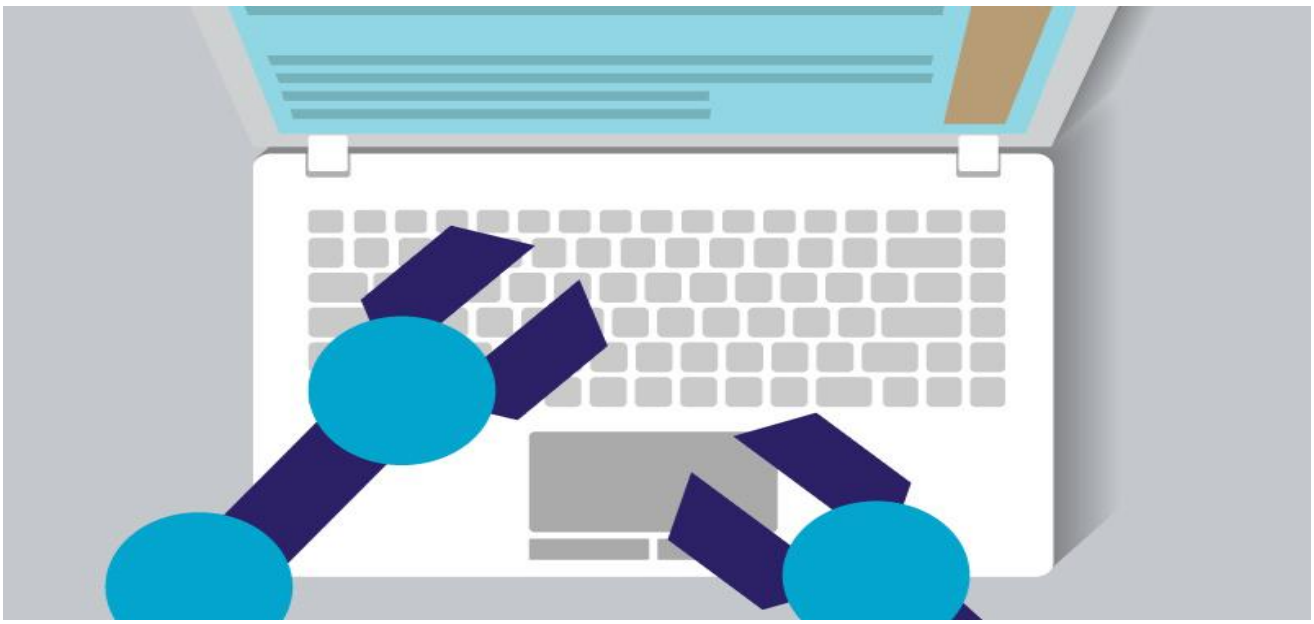
Figure 1 - Measured Local Ad Spend, Online vs. Traditional (Offline)



Note: Numbers are rounded.

Source: BIA/Kelsey U.S. Local Media Forecast 2017

Two solutions for reaching local audiences are (1) programmatic geotargeting and (2) buying media directly from local outlets. For example, an advertiser might make a geotargeted buy in programmatic exchanges targeting audiences in local markets. Or the advertiser could buy directly from local media in those markets. In each case the goal is delivering ad impressions to locally targeted audiences. What's the difference?



Programmatic Geotargeted vs. Local Direct Media Buying

It turns out that, from an ad fraud perspective, there are different levels of risk with geotargeted programmatic versus local direct media buys. It's entirely a matter of economic incentives and where fraudsters gravitate to find the bigger and relatively easier money. While the publishers participating in programmatic obviously include legitimate and high-quality environments for advertisers, unfortunately, this is an environment that attracts criminals.

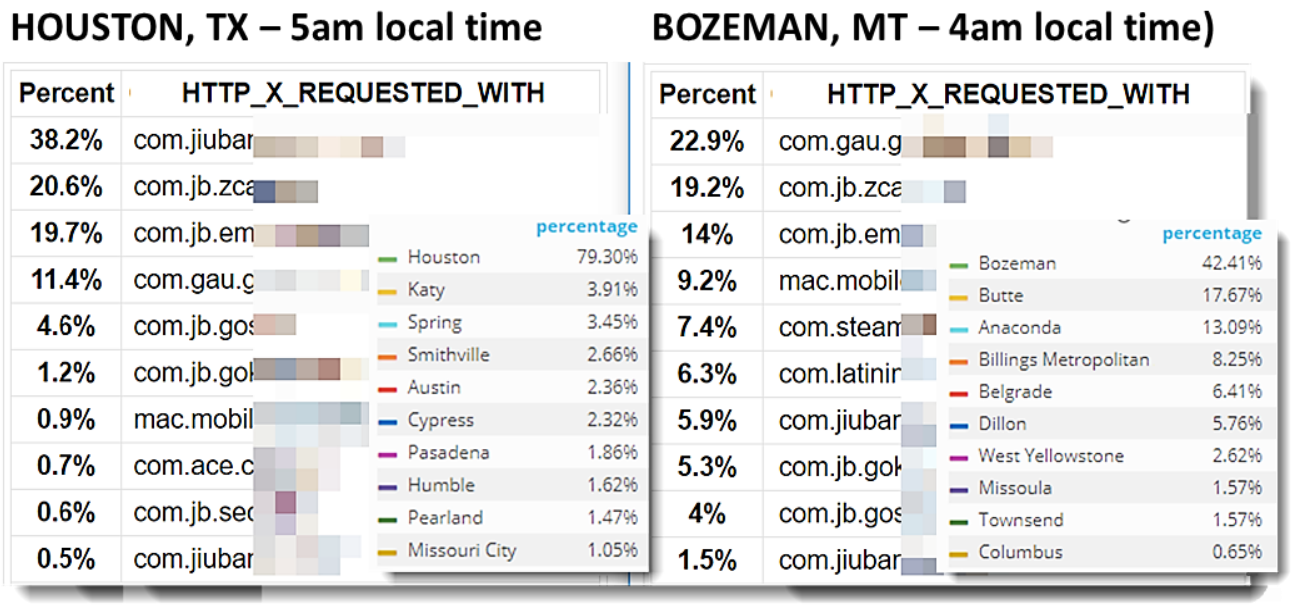
The basic mechanism of ad fraud is bot-driven non-human traffic that mimics humans. It is becoming increasingly sophisticated. Ad fraudsters can participate in open programmatic exchanges by fraudulently marking up their messages to appear as a legitimate publisher site offering audiences in the targeted geography. Essentially, a fraudulent company can set itself up with a seat on programmatic exchanges and offer fake inventory to advertisers by claiming to be a legitimate publisher. Once a buy/sell transaction occurs, the fraudulent site accepts the ad placement and then uses bot technology to simulate actual audience behaviors, e.g., clicks, views, downloads. The advertiser pays the bill and receives encouraging but false reports about audience engagement.

Furthermore, fraudsters are honing-in on mobile and geotargeted campaigns because those typically have higher CPMs and are less measurable by traditional ad fraud detection technologies that rely on javascript data collection. In-app impressions are not measurable by these fraud detection technologies. Fraud apps combine with fake devices in a potent cocktail to defraud marketers. The fake devices can pretend to be in any geolocation – country, state, city, DMA, etc. – and the apps can rack up millions of impressions in minutes. Considering that more than half of digital ad spend is already in mobile, a lot of dollars are at stake. (See: At Scale Ad Fraud Absorbs Most Digital Dollars).

Test Case #1: Suspected Ad Fraud in Butte-Bozeman and Houston Markets

To test this hypothesis, we decided to conduct a "natural experiment." We compared mobile ad performance from a programmatic campaign targeting Houston to another arbitrary, tiny market unlikely to match Houston – Butte-Bozeman, MT.

Figure 2 - Comparison of Geotargeted Programmatic Buys in Two Local Markets

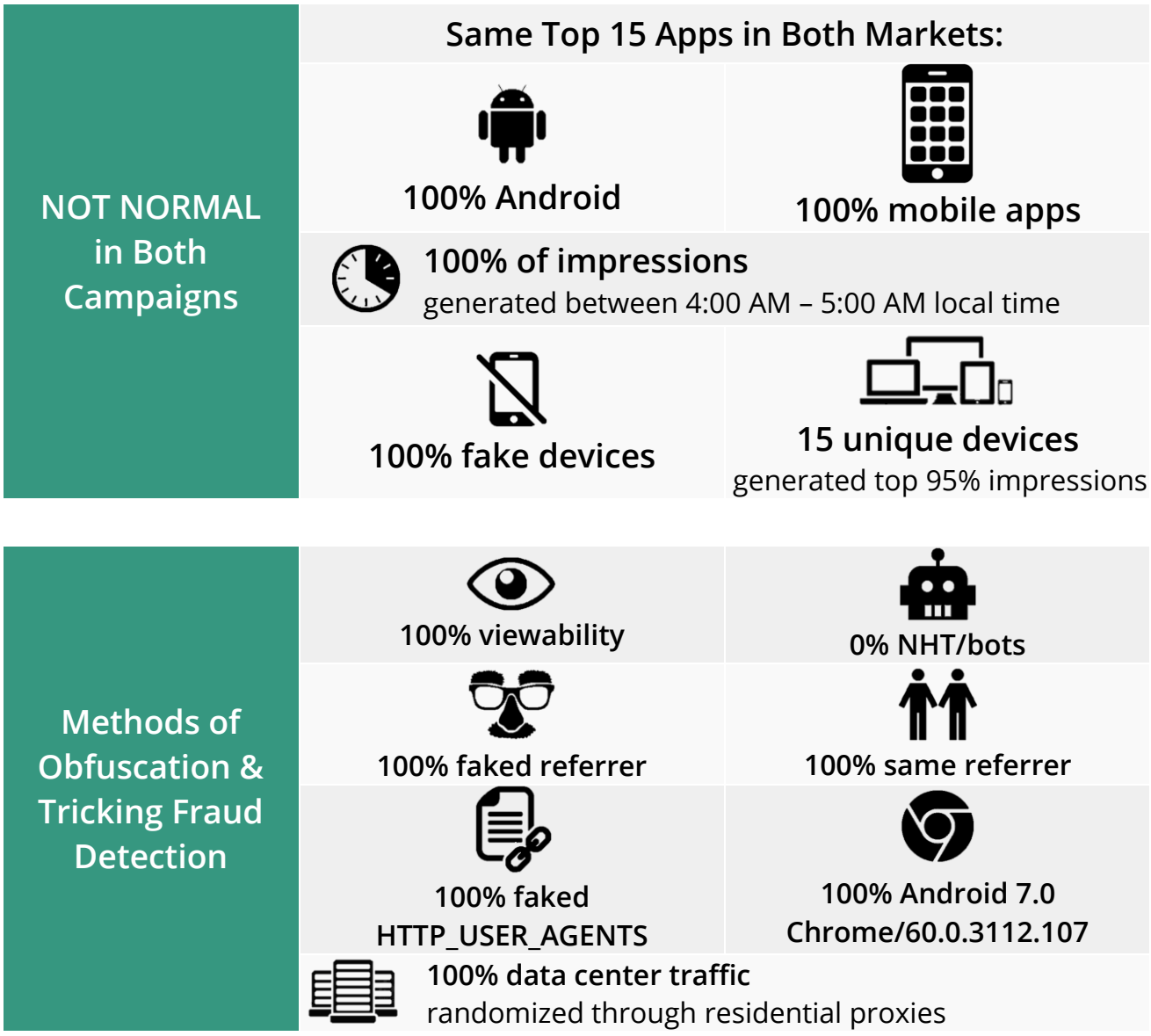


Source: BIA/Kelsey and Marketing Science Consulting Group

The programmatic campaigns specifying Houston and Butte-Bozeman geographies were faithfully executed by the exchanges but the results delivered aren't logically possible. For example, 100% of the devices were Android, unlike a normal distribution that includes iPhones, iPads, and other types of devices. 100% of the ad impressions were generated at 5:00 AM

Houston time and 4:00 AM Bozeman time, respectively. There was 100% overlap in the mobile apps that caused the ad impressions – that is, the same apps generated the ads in both markets at the same time. None of these apps are mainstream, or likely to be used by humans. Based on these observations and many others, these ad impressions were deemed to be fraudulent, and not loaded by real humans, using mobile apps, in those geotargeted locations.

Figure 3 – Key Findings

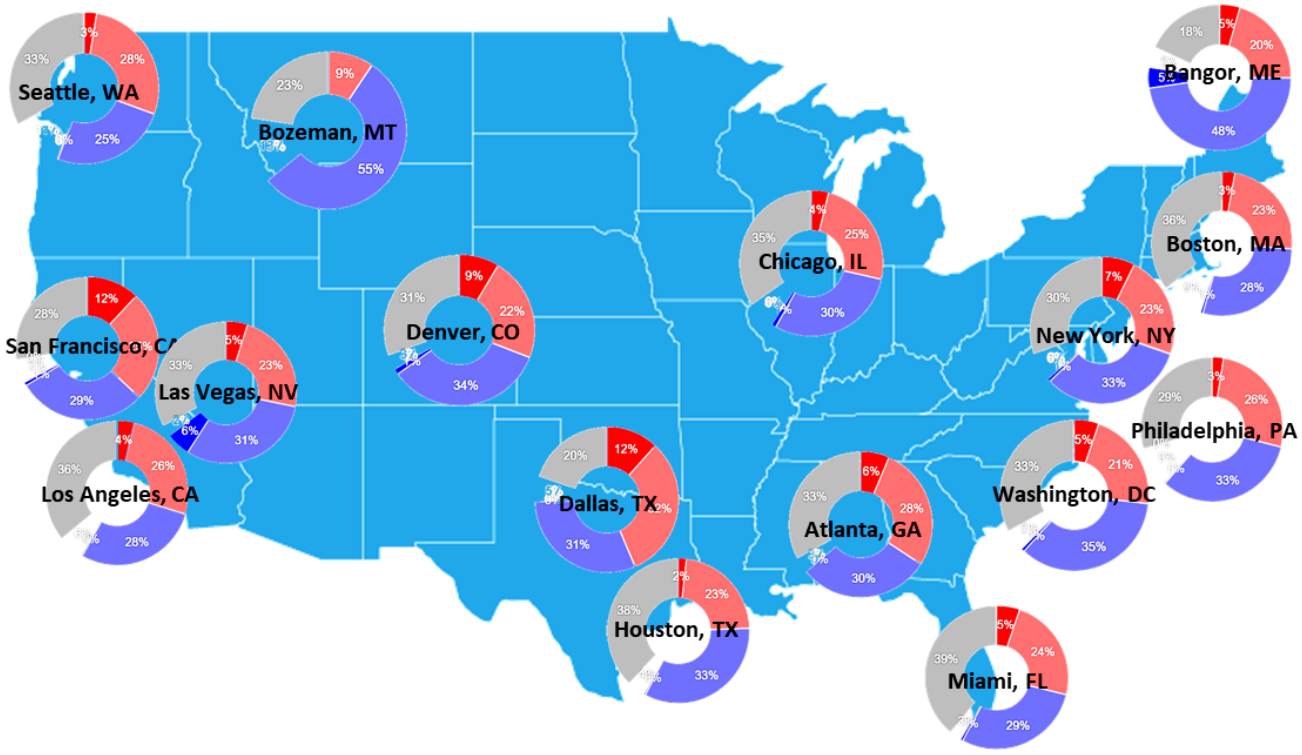


Source: BIA/Kelsey and Marketing Science Consulting Group

Test Case #2: Expanded Experiment to 16 DMAs Across the United States

BIA/Kelsey and Marketing Science then expanded on this initial test to include the geotargeting of 16 DMAs through programmatic media buying.

Figure 4 - Relative Ad Fraud Levels in 16 DMA Geotargeted Programmatic Media Buy



Source: BIA/Kelsey and Marketing Science Consulting Group

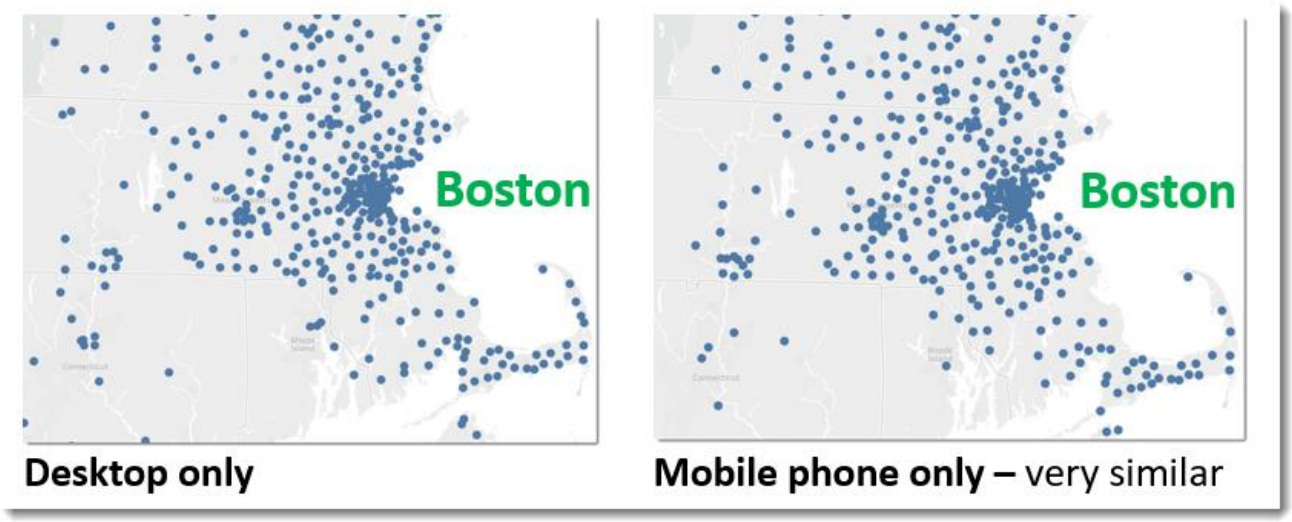
The resulting data showed that while there are variations in the levels of fraud between DMAs (Figure 4), the differences are insignificant and not actionable. For example, the fact that San Francisco and Dallas have higher rates of fraud than other DMAs (dark red in the overlaid doughnut charts) does not mean marketers should spend more or less in those markets.

Figure 5 - Map of Ad Impression Locations from 10 Geotargeted Programmatic Campaigns

Source: BIA/Kelsey and Marketing Science Consulting Group

Furthermore, when plotting the visit data on a map, we can show that the targeting by geolocation worked well, generally. The clusters of data points were centered around the 10 DMAs that were specified in the campaign targeting. But notice that there were also distinct data points outside those geographies (identified by red rectangles). These represent data center locations and Internet gateways or simply unknown geolocations based on the IP address.

Figure 6 - Close-up of One DMA – Geolocations of Desktop and Mobile Users



Source: BIA/Kelsey and Marketing Science Consulting Group

It was also clear that the geotargeting based on IP address locations are coarse – not very accurate. As seen in the pair of charts above in Figure 5, this "coarseness" appears as "freckles" in both desktop visits and mobile visits. These are geolocations estimated from the IP addresses of the visitors, NOT obtained from real GPS locations, for both desktop computers and mobile devices. The real GPS locations from the mobile devices were not used.

As such, the geolocation data used for targeting in programmatic exchanges may be good enough for certain types of marketing campaigns – like ones broadly targeted at entire cities or DMAs. But they may not be suitable for other marketing campaigns that require more accurate and fine-grained locations, for example, based on real GPS data from mobile devices.

The key takeaway here is that fraudsters can target local ad spend by providing faked geolocation data and selling such ad inventory through programmatic exchanges. Marketers trying to target local audiences should also consider buying direct from local media publishers – for example, placing ads on local TV, radio, newspaper, and magazine websites. The key difference is that the local media outlet sites are visited by humans that live in those locations, as opposed to targeting users based on geolocation information that may show they are in those locations.

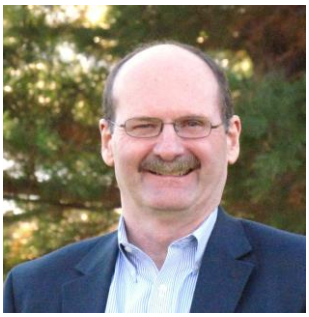
Early Conclusions and Recommendations

1. **Programmatic Geotargeting vs. Local Direct Media**: Ad fraud is dependent on the way the media is bought -- programmatic geotargeting vs. direct buys with local media outlets. Buying direct from local media may result in much higher quality (more human vs. bot) audiences.
2. **Ad Fraud Variance Across DMAs is Not Actionable**: While we see a range of the relative levels of ad fraud traffic from 2-12% across DMAs, we don't feel the variance is significant or actionable; the levels of fraud depend on which ad exchanges and sites actually ran the ads.
3. **Geotargeted Ad Fraud is a Scaled Problem**: It appears that in the very best-case scenario, about 6% of ad campaign traffic in programmatic exchanges for DMA-level geotargeted campaigns is fraudulent, non-human bot traffic. This both "steals" ad revenue from publishers and it also negatively impacts campaign results and marketer. Worse yet, marketers typically expect ROI multiples for geotargeted campaigns, e.g., 5-30x increased response over non-geotargeted campaigns. This means that while an average of 6% of ad spend is wasted due to fraudulent bot traffic, the impact on ROI can be 5-30x worse.
4. **Ad Fraud Coming to Local Media**: Fraudsters go where the money is, particularly the easy money. As the general ad fraud "market" opportunities diminish, fraudsters may move to target local media ad dollars and tap into this market.

About the Authors

RICK DUCEY

Managing Director
BIA/Kelsey



Rick Ducey is managing director, leading BIA/Kelsey's strategy consulting practice. He assists clients with their business planning and revenue models, strategic research, market assessment, and designing and implementing strategies for leveraging video media assets and inventory in local markets. 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 joining BIA/Kelsey in 2000, Ducey was senior vice president of NAB's Research and Information Group. Ducey was recognized in academia as the 2011 Shapiro Fellow at George Washington University, where he teaches entrepreneurship in new media. He has also taught on the faculties of Michigan State University, George Mason University and the University of Maryland. Ducey received his B.A. from the University of Massachusetts at Amherst, M.S. from Syracuse University and Ph.D. from Michigan State University.

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.

BRAD ADGATE

Executive Industry Advisor
BIA/Kelsey

With 35+ years of experience in the industry, Brad Adgate is a well-known media insights veteran. Adgate has worked at many top tier advertising agencies and media companies. These include working in the research departments at Grey Advertising, Backer & Spielvogel, Saatchi & Saatchi Compton, Horizon Media, LBS Communications, Turner Broadcasting, Westinghouse Satellite Communications, The Family Channel, and Comcast Spotlight. Adgate has been published by Ad Age, Adweek, Mediapost and is a contributor to Forbes.

Adgate has been a member of several advisory boards and committees, including the Council for Research Excellence in which he chaired the Digital Committee, the Board of Directors of the Media Rating Council, The Board of Governors of the Advertising Research Foundation as well as on the advisory boards for Nielsen's Local TV Committee, Arbitron Radio and Kantar Media. Adgate had also occupied the chair of the American Association of Advertising Agencies (4A's)'s Media Measurement Committee.

Adgate is a graduate of Jacksonville University with a bachelor's degree in history and political science. In 2014, he was named "One of 80 Alumni You Should Know" by the university.

More Local Advertising Research

This report and much more of BIA's local advertising research and analysis available in:

BIA ADVantage

Realize local advertising revenue with BIA ADVantage

BIA ADVantage is an online dashboard that provides extensive, quality data along with expert analysis to reveal the advertising trends and opportunities in local markets and nationwide.

Learn more at https://dashboard.biakelsey.com.

Interested in a demo? Email advantage@biakelsey.com.

About BIA/Kelsey

BIA/Kelsey is at the forefront of local media analysis, creating and delivering unique data to examine traditional and digital advertising, advertiser trends and activities, local market profiles and station ownership/operational details.

We offer comprehensive local and nationwide advertising research, competitive intelligence services and strategic and valuation consulting. New for 2017 is our advertising dashboard - **BIA ADVantage** - that provides direct access to our comprehensive industry intelligence and quarterly briefings.

For clients, our promise is to combine quality data with high-powered analytics to help them capitalize on new sources of revenue and make smart, better decisions. broadcast.biakelsey.com.

Additional information is available at:

- www.biakelsey.com
- Local Media Watch blog
- www.twitter.com/BIAKelsey
- www.facebook.com/biakelsey
- BIA/Kelsey's Local Media & Technology Daily Newsletter