collective wisdom®

SZABO ASSOCIATES, INC. VOLUME 29, ISSUE 3, SEPTEMBER 30, 2014

Dear Friends:

How things can change in a few short years! Most major U.S. media companies today sell advertising space using some sort of programmatic means—98.3% of those recently surveyed by the Interactive Advertising Bureau and the consultancy Winterberry Group. Automated tools and software for making online buys have created new avenues of opportunity for media. Unfortunately, they have also created new opportunities for fraud. This issue continues our Q & A's by exploring the serious problem of traffic fraud in digital advertising. We also discuss the impact of consolidations among media companies and agencies, as well as the changing customer base.

Our fall calendar of events includes the BCCA (the media industry's credit association) Media Credit Seminar, November 6 in New York, New York; and the Szabo Holiday Party, December 13 in Atlanta.

Best wishes for a fine fall season,

Robin Szabo, President
Szabo Associates, Inc.

Questions and Answers Part 2 . . . Fraud, Bots, and the Changing Customer Base

As the saying goes, every choice carries with it a consequence. The digital marketplace, while rich with opportunity for media and their customers to make money, is also rich with opportunity for criminals to do the same. Traffic fraud is a serious problem that needs to be successfully attacked to preserve the integrity of interactive advertising.

Consolidations among media companies and agencies continue to alter the advertising landscape. Media's customer base is also changing. Among the multitude of choices available to advertisers are opportunities to inexpensively create online marketing avenues for themselves.

Traffic Fraud.

Question: As we expand our media business to include digital advertising, our customers are expressing concern about the possibility of illegal activity that can lead to false performance data. What are the motives and methods behind this kind of fraud?

The motive is money, and lots of it. The perpetrators are professionals, who often operate from overseas and engage in numerous forms of organized criminal activity. They look for opportunities in areas that are vulnerable and resist detection. Because its performance metrics are vague and systems are easily infiltrated, digital advertising—including online, social, and mobile—is an attractive target. Digital ad placements purchased through exchanges and even directly from publishers can be subject to infiltration. According to recent estimates by the Interactive Advertising Bureau (IAB), about 36% of all Web traffic is considered fake.

How the Crime is Committed. The criminals use code to create fake "robotic" traffic, called "bots," which simulate human behavior. Clever bots may "click" through to websites, but the trip ends there. No real engagement takes place, and no purchases are made; however, significant damage is already done. The intent is to fool both buyers and sellers into believing the results, or metrics, are better than they really are. Because only humans can generate real results, the effect of these robotic actions is to corrupt the engagement metrics driven by human interaction.

The IAB offers the following example to show how easy it is to become a victim of traffic fraud: A user clicks on a link that takes him to a compromised site, or he is tricked into downloading software. This action infects his PC with a malware virus, which turns it into a "zombie" or "node" on a bot net. Meanwhile, a bot net controller (the criminal) hosts an "advertising impressions storefront" on the Web, promoting the sale of "real unique visitors to your website." A website or network owner, in an attempt to drive traffic, buys impressions from the storefront with a credit card. The money flows to the criminal, who starts

—continued on page 2

Questions & Answers—

—continued from page 1

sending bot traffic through the nodes in the bot network (remember the infected PC?), driving fake impressions to the website or network. The website or network owner's reporting shows that impressions have hit the site and clicks have occurred, and he is unaware that these activities have been bot-generated.

Bot code may create false traffic in several ways, according to the IAB. It may generate ad views while consumers browse unaware. The consumer cannot see these ads because they are hidden behind other ads or content, displayed in tiny iFrames, or served in other ways that prevent them from being observed. The bots may take over user controls to generate false clicks when the computer is not being used. They may also run unseen processes to simulate consumer activity or compromise cookie data to look like high-value consumers.

"Impression laundering" makes impressions generated by bots, impressions generated on rogue sites, or impressions of the wrong type appear to be legitimate. It does so by concealing the actual URL where an ad appears by using "front sites" that mask themselves as legitimate publishers. According to DoubleVerify, a company that offers transparency and accountability solutions for digital advertising, programmatic buying is particularly vulnerable to this type of fraud because of what it terms the "Transparency Gap." In programmatic buying, the transaction URL often ends up being different from the true URL because of the numerous handoffs required to process the request. While many of these mismatched URLs occur for legitimate reasons, this gap creates an environment that is rife with hiding places for fraud. DoubleVerify asserts that nearly 90% of fraud appears in the transparency gap of programmatic buying.

The Fallout. Advertisers generally pay for ads that are loaded when a user visits a Web page. If a human user is indistinguishable from a non-human user, the marketer ends up paying for eyeballs that were never there. When ad performance fails to meet their expectations, and/or fraud is suspected, advertisers may abandon or cut back digital media buys.

Legitimate businesses, including media, can easily fall prey to fraud. Purchasing traffic is a generally acceptable method for publishers to extend audience and increase inventory. By unwittingly buying traffic from fraudsters, media can compromise their available inventory and hurt their relationship of trust with customers.

Bot fraud has also helped to spawn anxiety among advertisers about other areas of ambiguity in their ad buys. According to a recent survey by the Association of National Advertisers (ANA) and Forrester Research, transparency issues are on the rise, with 46% of marketers expressing concern. The areas of concern most frequently voiced are the reliance on served rather than viewable impressions, how and where digital advertising gets placed, lack of visibility into data used to define audience targeting, and lack of information about pay arrangements between agencies and media sellers.

As reported recently in the *Wall Street Journal CMO Today,* revelations of ad fraud in the programmatic sector is causing marketers to voice concerns about how their agencies' programmatic specialty divisions, called "trading desks," actually work. According to *WSJCMO,* some trading desks buy online media inventory and then resell it to their advertiser clients. The fee charged is not based only on the cost of the ad space; rather, the space is bundled with data and technology to arrive at the fee. Clients cannot always see what part of their ad budgets is going to ad space and technology and what part is going to the trading desk.

Question: Is traffic fraud a problem that carries shared responsibility? What can we do as credit and collection managers to assure our customers that their data is authentic?

All parties in the media buying chain should assume some responsibility in order to protect themselves and to help eradicate these unlawful and destructive operations. Both traffic fraud and transparency issues must be addressed to preserve the integrity and value of digital advertising for all participants. Only through collective and concerted efforts by marketers, publishers, and targeting providers will the bad actors be eliminated.

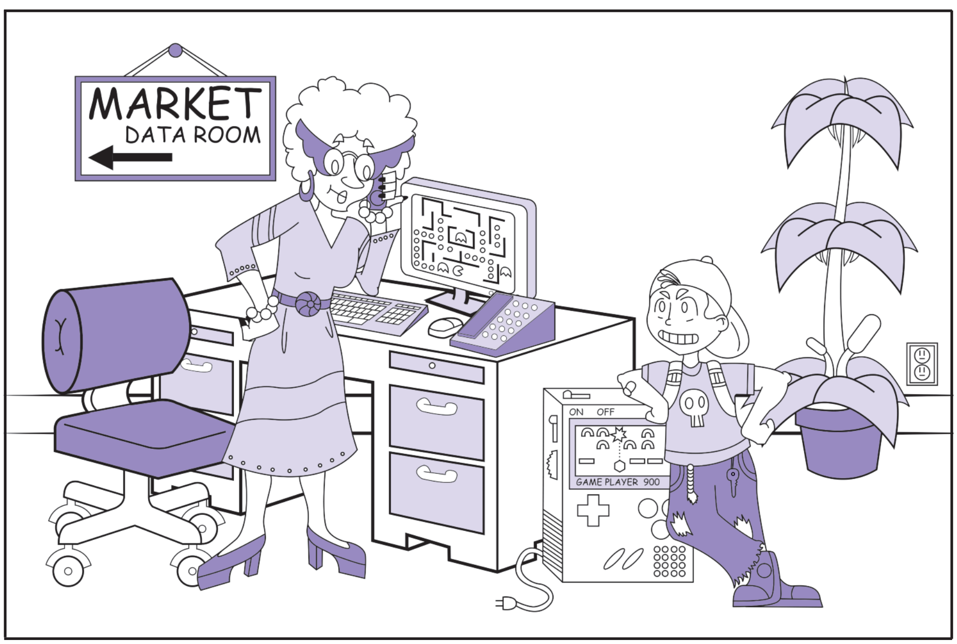
The Industry vs. Evil Bots. The IAB announced last year the formation of its "Traffic of Good Intent Task Force," composed of 41 member companies and other key contributing companies, whose mission was to formulate ways to combat traffic fraud. The organization issued its final version of "Traffic Fraud: Best Practices for Reducing Risk to Exposure" in January 2014. The document, available on the IAB website, urges the industry to actively address the threat and offers best practice procedures for publishers, networks, and buyers of digital advertising. While it recommends that publishers avoid purchasing traffic, which may put long-term success at risk for short-term profits, the organization recognizes that you may need to increase inventory and presents guidelines to help mitigate the risks.

To Catch a Thief. Other industry participants are actively pursuing ways to fight bot fraudsters. In July, the ANA and online fraud detection firm White Ops announced a joint research initiative to determine the level of bot fraud across the digital advertising industry. Its goal is to "provide actionable data and insights which marketers can use to reduce bot fraud in their future campaigns." Thirty ANA big-brand member companies, covering the spectrum of consumer marketing, are posing as unsuspecting advertisers in a sting operation that commenced in August. White Ops has tagged each brand's ads with code capable of identifying bot fraud. Each participant will receive a customized confidential report providing overall fraud rates, fraud by platform (desktop, mobile), format (display, video), channel (publisher, network, exchange), and other relevant findings. The aggregate study results and recommendations will be available to the industry in the fourth quarter of the year. Other industry players as well are contributing to the fight. For example, DoubleVerify announced in June that it had uncovered a significant video ad impression laundering scheme.

What to Do. Through trade and industry organizations such as ANA and IAB, savvy buyers are learning about and investing in ways to maximize the quality of their digital advertising. Publishers must look at their methods from their customers' points of view and take actions to allay concerns as much as possible. The IAB recommends that premium publishers pay a higher price to buy quality; look for a natural affinity between their content and the purchased audience; use technology to detect non-human traffic; keep standards high if and when performance falls below goals; and know their consultants and where they are sourcing traffic.

The IAB Best Practices document includes questions to ask your sources of inventory, which correlate to the questions it recommends that buyers ask you. In general, you should use only traffic sources that have their audiences measured by verifiable third-party vendors, which allow advertisers to compare their ad-generated traffic against an independent benchmark. Not all measurement techniques are created equal however, and these methodologies need to be compared. Your website should have a policy and technical methodology to distinguish between human and non-human traffic as well as processes for removal. The site URL reported by first-and/or third-party campaign performance analytics should correspond with the URL on traffic-sourced sites. Your site should also actively screen for malware, monitoring traffic patterns in real time to recognize irregularities.

Visit the IAB website regularly for additional information and updates. Keep abreast of new advancements by companies that provide technology solutions to bot fraud. Perpetrators of fraud will continue to work on ways to undermine efforts to crush them, so media need to stay tuned in to stay on top.



"Boss, Mr. Simmons heard about those 'robots' that can mess up his marketing data. Says his grandson is mighty good at blowing 'em to bits. Should I send him on up?"

Mergers and Changing Customer Base.

Question: We are seeing media companies' and agencies' efforts to change and even merge into bigger organizations. Should these developments affect the way our own credit and collections department operates?

Changing technology has made old business models obsolete, and shake-ups are occurring in all areas of the industry.

Merger Mania. This is the era of mega-mergers in the media industry. Cable and satellite television providers are consolidating, giving them increased leverage when they negotiate for programming. Some media companies, feeling threatened because they need to realize a certain revenue from the programming they provide, want to increase their clout by getting bigger too.

The principle also holds true for advertising agencies. If one huge company is selling time/space for a large group of properties, agencies may feel the need to band together to acquire sufficient client buying power. Additionally, with programmatic buying and selling of online advertising, along with powerful analytical services and software to help advertisers get the most for their advertising dollars, agencies are losing some of their value. Some advertisers are dispensing with agencies altogether, creating their own campaigns in-house and even operating their own trading desks. Subsequently, agencies are seeing the need to redeem lost value by providing their clients with technology to automate the buying process, which only sizable agencies can afford to implement. They are also hoping perhaps to persuade their clients that they can negotiate better rates than the clients could do on their own.

Some organizations are choosing to carve off assets, sometimes to facilitate mergers. Both Gannett and Tribune split

—*continued on page 4*

SZABO ASSOCIATES INC. szabo MEDIA COLLECTION PROFESSIONALS

Collective Wisdom® is a publication of
Media Collection Professionals,
3355 Lenox Rd. NE, Suite 945, Atlanta, Georgia 30326
Tel: 404/266-2464, Fax: 404/266-2165
Website: www.szabo.com
e-mail: info@szabo.com

PRESORTED STANDARD
U.S. Postage PAID
Atlanta, GA
Permit No. 747

Questions & Answers—

—continued from page 3

broadcast and digital assets from their newspapers. Similarly, Journal Communications and E.W. Scripps announced plans to merge by putting newspaper and broadcast assets into separate companies.

Other consolidations address the concerns of advertisers with regard to fraud, ad verification, and viewability tracking. Google acquired the anti-bot firm Spider.io. As reported in *WSJCO,* comScore, a tech company that analyzes digital traffic, has acquired the anti-fraud firm MdotLabs. *WSJCO* states that such alliances also address advertiser and publisher complaints that they need to employ numerous vendors just to run a few ads.

Implications for Credit and Collections. The growth of online advertising is undoubtedly having an impact on the makeup of your customer base. You may be seeing fewer small and marginal customers because they are taking advantage of less costly do-it-yourself opportunities for "couponing" and other forms of digital advertising.

Agency consolidation may result in your having to manage fewer agency clients. These agencies generally are solvent and stronger as a result of consolidation, so your risks may have actually lessened. Some advertisers who previously placed ads through agencies may now deal directly with media. Understandably, advertisers are getting more assertive in monitoring what they are buying and receiving. Some are even modifying their contracts to hold publishers and exchanges accountable for bot traffic, and providing for make-goods or reimbursement if fraud is uncovered.

Service consolidations (shared service agreements) are becoming increasingly common among media properties and can have a significant impact on credit and collections. A company that owns a local network affiliate may also oversee operations of another network's affiliate in the same locale through a shared service agreement. Not all shared service centers are the same. Some do everything—credit, collections, billing, etc.—while others may do credit investigation but not collections, except on an as-needed basis. Those that do collections often start late in the process, making successful collection much more difficult.

Here are a few tips for dealing with challenges associated with the changing market:
1. Stay current on mergers and acquisitions. 2. Stay abreast of changes in agency contracts, including payment liability clauses. 3. Perform credit checks on new direct advertisers. 4. Study contracts for inclusion of clauses holding media liable for fraud. 5. Litigation costs are high, and commercial litigation attorneys are few, so consistently adhere to your collection policy and procedure schedule! ♦