Mindy Charski

TECHNOLOGY AND TRANSPARENCY IN THE FIGHT AGAINST AD FRAUD

'YOU KNOW DEEP DOWN WHEN YOU'RE BUYING SOME VERY CHEAP TRAFFIC— THERE'S SOMETHING NOT RIGHT ABOUT IT.'

Identity theft and credit card fraud make the headlines for their damage and deception, but there's another putrid kind of fraud that, according to Hewlett Packard Enterprise's "The Business of Hacking," requires less risk and effort and has a higher payout potential: ad fraud. The chicanery is rampant throughout the digital advertising ecosystem and has many different varieties. And while it's true that many players in the supply chain have incentives to ignore the problem, there's a growing momentum to stop ad fraud's costly creep.

Technology is an important weapon in the fight, but experts say combating ad fraud will also require buyers, sellers, and the companies in between to have smart business practices. For online publishers, those practices largely pertain to two issues: traffic bought through third parties and transparency for ad buys.

THE THREATS OF THIRD-PARTY TRAFFIC

Sourcing traffic is common in digital advertising, but it doesn't necessarily have the attention of many marketers, according to the white paper "Sourced Traffic: Buyer Beware!" from the ANA (Association of National Advertisers). It found that 61% of marketers were either slightly familiar or not at all familiar with sourced traffic, and only 19% were either very familiar or extremely familiar.

The paper explains the visitor acquisition arrangement this way: "With sourced traffic, a publisher pays a third-party vendor to send users to its site by advertising on other publishers' sites." Problems arise when users aren't actual people, but rather bots that can mimic human behavior. Advertisers end up paying for ad impressions served to those bots.

"When we talk about ad fraud, we're talking about fake web views that increase the number of ads served, making it look like there are more people browsing the net than there really are, which artificially inflates the supply in this market," says Michael Tiffany, CEO and co-founder of the security company White Ops.

To be sure, publishers often have no hand in the bots that visit their sites. The software may stop by to collect

cookies and cause the ad impressions to load somewhere else—often on fake sites awash with bot traffic that compete for ad dollars with legitimate sites. But publishers increase the chances that bots show up on their properties when they buy traffic. The "2015 Bot Baseline" report from White Ops and the ANA found that sourced traffic was more than three times more likely to contain bots than unsourced traffic. The practice can ultimately affect many kinds of buys, including direct, private marketplace, and open exchange programmatic.

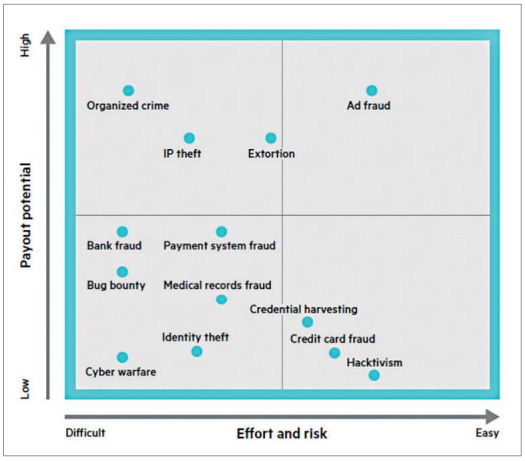
The notion that bought traffic would have more bots than organic traffic makes perfect sense to Augustine Fou, an independent ad fraud researcher. "There aren't a whole bunch of humans sitting around with nothing to do but to go to websites that you tell them to go to, so how are you able to generate 10 million ad impressions from a small site that has practically no content that humans want to see? When you buy it, that means they use bots to generate all that traffic for you," Fou says.

Ad fraud researcher and consultant Shailin Dhar adds, "You know deep down when you're buying some very cheap traffic—there's something not right about it." Still, pricing alone isn't a good gauge of traffic quality. Expensive traffic can be filled with bots too.

HARD HABIT TO BREAK

Simply not buying sourced traffic sounds as if it's an ideal solution for content providers, but it's complicated. Publishers often seek to acquire visitors for their sites because their own organic traffic isn't enough to meet the audience delivery requirements of an advertiser, according to "Sourced Traffic: Buyer Beware!"

It could start with a single purchase that performs really well. "That is a slippery slope you never want to start going down," Fou says. "Once you start buying traffic, you can't stop. Just imagine you show your boss that you got more traffic and higher ad revenue quarter over quarter, and then all of a sudden you stop buying the traffic. It's going to make you look really bad."



Source: "The Business of Hacking," Hewlett Packard Enterprise

In its white paper "The Business of Hacking," Hewlett Packard Enterprise finds that ad fraud—which it defines as "deliberately attempting to serve ads that have no potential to be viewed by a human user"—is generally more profitable and easier to commit than other types of fraud.

Also, there are the complexities of competition. "Any publisher paying attention knows how pervasive traffic sourcing is, which means there's a strong incentive for everyone to do it," says Tiffany. "If you know all your peers are doing it and getting away with it, then they can effectively undercut you on price or sell more volume than you—and that puts people at a competitive disadvantage in this world where the playing field's not even."

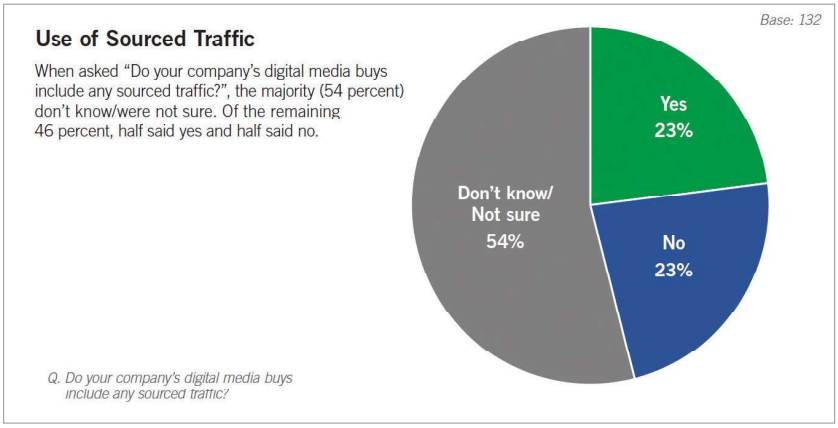
> 'It encourages publishers to really know what's going on in their own backyard. ...'

Publishers may also find they have a bot predicament when they use a related technique called audience extension in which they fill advertiser campaigns with inventory from other sites, incuding some on open exchanges. "The problem becomes, are you actually sure the demographics and the data [are] correct and you don't have a lot of bots pretending to be those humans?" Fou asks. "Audience extension has been a convenient euphemism of, 'Let's find these other audiences that go elsewhere,' and the 'elsewhere' happens to be all these bad sites. When you find an extension of your audience, you're allowing more fraud to creep in."

BOT MONITORING: IMPORTANT, BUT COMPLICATED

It's possible to monitor traffic for bots. Fou says publishers can also create filters that, when recognizing a bot, either allow the pages to serve without calling ads or prevent the page from loading at all so bots can't grab a cookie. Today, many proactive publishers are just at the monitoring stage, with fewer at the "filtering or blocking" stage, Fou says.

Monitoring is an important step, though—it is only through monitoring that publishers can understand how clean their traffic is and which third-party sources are bot-heavy and should be replaced. Frank Amorese, senior media director at HEINEKEN



Source: "Sourced Traffic: Buyer Beware!" by the ANA

An ANA white paper found that many marketers are unaware their digital media buys include sourced traffic. "We find this lack of familiarity and transparency disturbing," the association says in "Sourced Traffic: Buyer Beware!"

USA, says more publishers should have partners verify their traffic and should guarantee that advertisers are not paying for fraud. "I don't think the community at large [of advertisers] is putting enough pressure on publishers to do that," he says.

And yet, Amorese says advertisers should employ their own third-party verifications too, as HEINEKEN does. Otherwise, he says, "It's kind of like asking someone to grade their own homework. If there's a grey area, [publishers] would probably give themselves the benefit of the doubt." Amorese likens it to the use of a third-party ad server. "We want to make sure we have a third party there verifying the plan delivery that was agreed upon," he says.

However, problems can arise when publishers and advertisers independently use traffic monitors since they're likely to have different methodologies. The overlap may not produce the same results, and legitimate web traffic can be falsely identified as suspicious, Tiffany states, which produces reconciliation problems.

He says the industry's currently in an "awkward period where the [bot detection] standardization in this field is so new" and predicts it might take time for the industry to come up with a sustainable solution to prevent false positives.

INDUSTRY INITIATIVE LAUNCHES ANTI-FRAUD CERTIFICATION

Meanwhile, eliminating ad fraud is a top concern of the Trustworthy Accountability Group (TAG), which was formed in 2014 by three advertising trade groups: the ANA, the American Association of Advertising Agencies (4A's), and the Interactive Advertising Bureau (IAB). In May 2016, the initiative announced the launch of its anti-fraud certification program for direct buyers, direct sellers, fraud detection vendors and measurement services, and intermediaries. Participants must comply with guidelines relating to their specific roles in the supply chain.

Earning the Certified Against Fraud seal signals that a company is meeting the standard set by the industry and is doing its part to fight fraud, says Rachel Nyswander Thomas, SVP of operations and public policy at TAG.

For publishers, the requirements include complying with Invalid Traffic Detection and Filtration Guidelines (from the Media Rating Council, Mobile Marketing Association, and IAB), employing domain list filtering and data center IP list filtering, and following publisher sourcing disclosure requirements (PSDR). These disclosures about traffic sources can benefit both publishers and advertisers. "It encourages publishers to really know what's going on in their own backyard and to give buyers the transparency to make informed decisions about whether they are comfortable working with a publisher that has that level of sourced traffic," Thomas says.

> 'Transparency is also what is going to help us solve these problems and ensure we don't have a new set of problems facing us in the future.'

Likewise, the anti-fraud certification program can also help publishers find partners that are working toward establishing a cleaner ecosystem. "[Sellers] can be sure the folks to whom they are passing their inventory are also doing their due diligence," Thomas says. "That is why we built a certification that covers the entire supply chain with different roles depending on where you sit in that supply chain."

Getting verified by TAG—an initial requirement—and earning TAG certifications can cost thousands, but Thomas says the investment is worth it. "The lack of transparency is what has made it possible for

criminal activity to become embedded in a legitimate $50 billion supply chain," she says. "Transparency is also what is going to help us solve these problems and ensure we don't have a new set of problems facing us in the future. That's a pretty good reason for companies to be a part of the TAG community."

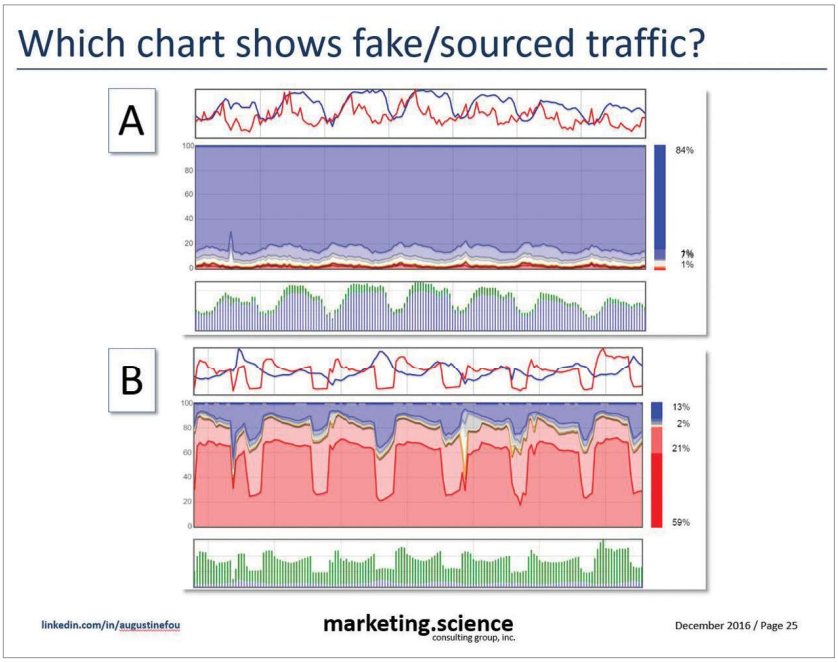
As of this writing, no publisher has earned the TAG Certified Against Fraud seal.

PREMIUM PUBLISHERS LAUNCH NEW AD MARKETPLACE

There are other collective efforts in the works, such as one from Digital Content Next (DCN), an association of premium publishers, which is constructing a digital advertising marketplace from the ground up. It's called TrustX and will operate as a public benefit corporation with no profit motives.

Advertisers can use the marketplace, which should start transacting early this year, to buy inventory from participating members. As of this writing, 27 publishers have signed on, including AccuWeather, Condé Nast, ESPN, and Univision.

Jason Kint, CEO of DCN, says building TrustX is a highly unusual step that goes beyond today's important cross-industry efforts of drafting standards, doing research, and talking about ad fraud. "Maybe we need something more here," Kint says. "An actual live marketplace where we can demonstrate what the right thing to do is for the advertiser, the publisher, and the consumer in a completely transparent fashion that's not trying to make money. Can we actually accelerate things [in terms of solving issues relating to fraud and transparency]?"



Source: Augustine Fou

This image helps us visualize what bot traffic looks like. Organic traffic comes into websites in smooth curves, but when bot traffic is turned on and off, it forms rectangular patterns.

The marketplace will use the analytics company Moat to filter out invalid traffic and measure human and viewable impressions. Advertisers will only pay for the ads that are seen by humans. Kint says for maximum transparency and trust, DCN is rethinking every element of the exchange through ad delivery. "We know the more companies, the more intermediaries, the more technologies that get inserted into the transaction, there's more vulnerability for fraud," he says.

ADVERTISER PRESSURE

It's worth noting that although there are technologies and business practices to help stop fraud, publishers can have incentives to not question the makeup of their traffic. "I think it is a publisher's role to not show ads to bots, but it's not in their financial interest to do so right now," Dhar says. That could change if they were able to demand higher cost per mille for their human visitors, he says.

Ultimately, it may be pressure from advertisers that gets publishers to take a more active stand against ad fraud. HEINEKEN, for instance, works with a number of verification companies to ensure it is getting the inventory it agreed to. The company won't pay for impressions that are fraudulent or not viewable. "We're very clear up front on what we want," Amorese says. "When people get the business, they understand how they're going to be measured—and if they don't live up to it, then they understand why we're optimizing out of them." EC

MINDY CHARSKI IS A DALLAS-BASED FREELANCE WRITER WHO HAS WRITTEN EXTENSIVELY ABOUT THE INTERSECTION OF BIG DATA AND MARKETING. ***COMMENTS?*** EMAIL LETTERS TO THE EDITOR TO ECLETTERS@INFOTODAY.COM.