

# ANA

Leadership and Marketing Excellence

TREACHERY

DECODING

FRAUD

IN

THE

DIGITAL

THE NEW SCHOOL  
OF TRAINING

SPECIAL SECTION:



BIG DATA'S ROLE IN  
DIRECT MARKETING

MARCH 2015



## The fraud-related danger marketers face in the digital age and what's being done to squash it

By Michael J. McDermott

For most marketers, digital fraud is something like a buzzing hornet in a busy room. It's distracting, you know it's there and can sting you, but swatting at insects is not high on your priority list. So you go about your primary business — brand building — and hope somebody else will take care of the little pest. Bad decision, as it turns out.

The digital supply chain is beset by serious fraud issues, including piracy, malware, lack of transparency, and perhaps most threatening, bot fraud. "It's at a point where less than 50 percent of dollars that marketers are investing in digital display and video are reaching the consumer," says ANA President and Chief Executive Officer Bob Liodice, citing an extensive report the association completed in partnership with White Ops, which specializes in deterministic botnet detection and digital fraud prevention. Representing projected losses of \$6.3 billion to advertisers







in 2015, that “little pest” is more like a master thief — with a hand firmly inserted in the marketing community’s pocket.

Some of the numbers in the ANA/White Ops study of bot fraud are staggering, none more so than this: Publishers

who purchased sourced traffic from third-party suppliers to drive additional unique visitors to their site sustained a bot fraud rate of 52 percent on that traffic. The numbers are less eye-popping, but still alarming, in other areas of online

marketing. Almost a quarter of video ad impressions in the study were identified as bot fraud, as were 11 percent of display ad impressions, while 17 percent of programmatic display bot traffic was fraudulent, and bot fraud for retargeted ads averaged 19 percent.

While the study found bot fraud in every domain category it examined, the highest levels occurred in the domains of finance (22 percent), family (18 percent), and food (16 percent). “That really jumped out at me, the fact that finance is one of the most polluted domains,” says Mark Clowes, global head of advertising at AIG. “The other thing was that so much premium and more-expensive inventory is at risk, which makes sense — the crooks are going where the money is.”

Like Clowes, Ron Amram, senior media director of marketing at Heineken USA, was aware of digital fraud’s growing threat prior to the release of the ANA/White Ops report, but he, too, sees it as a wake-up call. “I have to admit, I was a bit surprised by how much bot fraud was uncovered for some advertisers. Clearly, bot-related fraud is more systemic and pervasive than we anticipated,” he says.

“Gentleman hacker” Michael Tiffany, cofounder and chief executive officer at White Ops, says Clowes’s and Amram’s reactions are emblematic of the marketing community as a whole, which often views fraud as something that happens to other people. He finds that marketers assume fraud does not affect their premium buys purchased through premium channels. “Or they thought fraud was getting filtered out of their buys by their suppliers,” he says. In the wake of the report, the marketing community is now grappling with the fact that the huge amount of money pouring into online advertising has attracted the most motivated cybercriminals. “These botnet operators aren’t just preying on the lazy or inattentive. They are actively gaming

## TROLL TROUBLE

Entities that acquire patents (usually technology-related) with the sole intention of filing patent infringement claims against targeted users have become a growing problem in recent years. As President Obama observed in a 2013 White House report on patent assertion entities (PAEs), or, as they’re more commonly known, patent trolls, PAEs “don’t actually produce anything themselves. They’re just trying to essentially leverage and hijack somebody else’s idea and see if they can extort some money out of them.”

Last year, trolls were responsible for more than 60 percent of the patent cases filed in the U.S. [🐦](#), reports Daniel Nazer, a staff attorney and the Mark Cuban Chair to Eliminate Stupid Patents at the Electronic Frontier Foundation (EFF), a nonprofit advocacy group for user privacy, free expression, and innovation in the digital world. More telling is the growth in the number of unique defendants sued by trolls, which stood at 634 in 2004. “By 2013, that number had skyrocketed to 3,785, an increase of 600 percent,” Nazer says.

A couple of funnymen have emerged as the public face in the fight against patent trolls. Marc Maron and Adam Carolla are both comedians who launched successful podcasts and were subsequently targeted by a patent troll. Carolla settled with the troll last year, reportedly without paying any monetary damages, although terms of the settlement were sealed, while Maron fights on. But attacks by patent trolls are not limited to high-profile targets.

The White House report notes that PAE activities hurt firms of all sizes, and their suits increasingly target end-users of products, including marketers. “Unfortunately, there are so many bad software and Internet patents that it is almost impossible to avoid infringement,” Nazer laments. Marketing practices as mundane as using QR codes to direct mobile device users to web content and placing static ads in video streams have been targeted by trolls. “Since everyone engages in these practices, it is largely a matter of luck whether or not you get hit with a troll suit. The only real solution is reform of the system,” he says.

Efforts to achieve that reform are underway, and the EFF and other patent troll opponents are hopeful that meaningful legislation will be passed in 2015. In the meantime, marketers can take some steps to limit exposure, especially in the area of client/agency contracts. “This is an enormous problem. It has also led to liability issues as to who is really responsible for bearing the financial burden in patent troll cases,” says Bob Liodice, president and chief executive officer at the ANA.

In a white paper on this topic, the ANA recommends that clients generally not indemnify agencies for patent claims. “Rather, agencies should assume the liability for their work product, including liability for patent infringement. Accordingly, client/agency contracts should include ‘indemnity clauses’ which require that the agency step in and defend the client in the event of a patent infringement claim,” the report suggests. It adds that shared approaches to liability are gaining traction in the marketplace, and “ANA members are encouraged to consider whether a shared approach to liability makes sense in any of their agency relationships.”

— M.J.M.



# NATIVE ADVERTISING'S NEED FOR TRANSPARENCY

**F**or all the technological firepower being deployed on both sides in the digital fraud war, questions around the issue of deception in the area of native advertising serve as a reminder that new marketing opportunities still require tried-and-true measures of accountability. “The main concern here is whether or not deception exists, and if so, whether it can be eliminated by disclosure of the nature of the advertising,” says Reed Smith LLP partner John Feldman, who is giving a presentation on this topic at the 2015 ANA Advertising Law & Public Policy Conference later this month.

While it is not clear at this point whether there is a one-size-fits-all solution for accountability in this area, transparency stands as the touch word for all forms of native advertising, according to Feldman. “If in doubt, a transparent position will be the most conservative,” he says. “Beyond that, consistency will be important in order for a marketer to maintain a position as to when transparency is necessary and when it is not.”


Noting that there is currently some confusion among regulators as to whether sponsored speech is or is not deceptive,

Feldman stresses that context is important. “If a marketer is actually sponsoring speech and promoting its goods or services in a direct way, then the most important thing to do is to act in a way that discloses the payment. Transparency is the name of the game,” he emphasizes.

It is important that the law differentiate sponsored editorial speech from commercial speech, and that only the latter be subject to regulation for deception under the FTC Act, Feldman argues. “There is a danger that, in its zeal to protect consumers, the FTC will look at a financial contribution as a proxy for commercial speech, which is incorrect,” he says. For publishers, receiving compensation for writing articles on a particular subject is “a natural, legitimate, and significant income source” that increases the volume of editorial content and provides opportunities for advertisers who wish to place their ads near such content, according to Feldman, who adds, “Primarily, it is only when the editorial speech is actually an endorsement with an undisclosed material connection that the speech may become actionable under a deception theory.” — M.J.M.

the system from within, with bots that fake performance — and they’re doing it everywhere, not just on the long tail,” Tiffany stresses.

## SUBTERFUGE, DUPLICITY, AND DECEIT

The most glaring downside of digital fraud for marketers is, of course, the billions of dollars lost in compromised media investments, but it’s not the only one. “This kind of fraud means we get a less clear read on our campaigns and how they are working,” Clowes points out. With so many marketing campaigns highly dependent on accurate targeting, the inability to determine whether a click is generated by a human or a bot raises another significant obstacle. [The ANA/White Ops study highlights ad bots’ significant role in defeating user targeting efforts.](#)  Cybercriminals infiltrate home computers with malware. Since they are using the computers of real people who log in to email networks, participate in social media, and

conduct e-commerce transactions, bots not only blend in, but get targeted as being real people. Coasting on the credentials of the real users of those hijacked computers, bots click more often than real people — but not so much more often that they stand out. The most sophisticated bots move the mouse to put the cursor over ads, place items in shopping carts, and visit many sites to generate histories and cookies, all of which make them appear more demographically appealing to advertisers and publishers, the study found.

There is also a moral or ethical component to the damage done by bot fraud. “From a pure marketing perspective, our dollars are being wasted,” acknowledges Fernando Arriola, vice president of media and integration at ConAgra Foods. “But from a broader perspective, it is terrible that our industry is facilitating organized crime.”

Digital fraud even poses an existential threat of sorts, not just to marketers, but to all participants in the digital supply chain, Liodice asserts. “Everybody loses, short- and long-term, because if you

make the supply chain so unsafe, we are not going to go there. Why should marketers invest their money in a supply chain where half of it is going to unintended sources rather than reaching their customers?” he asks. “If this trend were to continue and marketers were to turn away from it in the same way they have moved away from radio and print, then not only would the digital sphere stop growing, it would in fact have the potential to decline.”

## CHALLENGERS, CHAMPIONS, AND ADVOCATES

As massive a challenge as bot fraud presents, it is not the only one marketers face in the digital sphere. Others include piracy, native advertising (see “Native Advertising’s Need for Transparency,” above), malware, transparency, and patent trolls (see “Troll Trouble” on page 6). In some cases these issues are related or overlap with each other. Meeting these challenges requires a cooperative effort from all corners of the marketing





Psst.  
Click here.  
It will be fine.  
Trust us.

community, and that's already underway. A key development is the launch of the Trustworthy Accountability Group (TAG), a cross-industry compliance organization to combat ad fraud, malware, and piracy. Backed by the ANA, the American Association of Advertising Agencies (4A's), and the Interactive Advertising Bureau (IAB), TAG will build upon the initial work done by the IAB Trustworthy Digital Supply Chain Initiative, an effort begun last year to bolster trust among consumers, marketers, and publishers, among others.

"Major stakeholders in the industry are well aware of the criminal activities that are impeding the growth of the digital media and marketing industries —

ad fraud, IP theft, malware, and more," says Randall Rothenberg, president and chief executive officer at the IAB. "The establishment of TAG is a direct response from the IAB, the 4A's, and the ANA, pooling our resources to eradicate this sort of malicious behavior."

Nancy Hill, president and chief executive officer at the 4A's, emphasizes the importance of the collaborative nature of this initiative. "The problem is so widespread and takes so many forms that it is almost impossible to contain." Each solution that has been introduced to combat fraud is only able to attack one sliver of the overall fraud pie. As a result, agencies and marketers who think they have a handle on fraud prevention most likely only have a small portion of it covered," she says. "Yes, agencies have some fraud prevention systems in place, and that's a good thing. They are like the police force with feet on the street. TAG is trying to reduce overall crime rates."


There will be four pillars to the TAG program: preventing fraud from getting into the digital advertising supply chain, rooting out malware, preventing traffic to sites with pirated content or content infringement, and increasing business transparency within the supply chain. TAG's two primary activities to achieve those goals will be issuing standards and business practices for all of the entities that operate in the digital supply chain and certifying companies that adhere to them, and developing tools, which include things like "unique identifiers" that can be used to track money flows and payments.

The first shot fired in TAG's war on digital fraud is an anti-piracy initiative that uses the Core Criteria for Effective Digital Advertising Assurance as a framework to designate trusted technology providers who can help protect advertisers from websites that facilitate piracy and counterfeit products. "For

advertisers, the process is simple," explains Venable LLP partner Stu Ingis, who led the cross-industry drafting of the Core Criteria. "Once the program is deployed this spring, advertisers and agencies can ask that their advertising partners use a Digital Advertising Assurance Provider to identify websites and properties that do not meet that advertiser's brand standards."

Ingis adds that the TAG initiative is getting a positive reception among digital supply chain participants outside the marketing community because it increases industry confidence in digital advertising. "There has been strong support from the ad tech and publishing communities, and it reduces the financial incentive for intellectual property theft, so content creators are supportive as well," Ingis says.

As important as industry-supported collective efforts such as TAG will surely be in the fight against digital ad fraud, Liodice insists that the support and involvement of individual marketers will be just as important. Marketers have a responsibility to "challenge the system," rather than just assuming everything is working the way it should. They must understand where their investment dollars are going and make sure they are truly optimal, and they must hold their partners to the same standards.

"Think about the ANA/White Ops study for a second. It contains a specific action plan for buyers, and just adopting some simple strategies, such as advertising during waking hours and demanding transparency for sourced traffic, can result in tremendous savings," Liodice says. "Don't shy away from these issues. There is an extraordinarily bright side to digital advertising, and we must not lose sight of that. But at the same time, we have to recognize the challenges we face and make a commitment to meet them head on." 

## AN ACTION PLAN FOR BUYERS

- ▶ Be aware and involved.
- ▶ Request transparency for sourced traffic.
- ▶ Include language on non-human traffic in terms and conditions.
- ▶ Use third-party monitoring.
- ▶ Apply day-parting when you can.
- ▶ Update blacklists frequently and narrowly.
- ▶ Control for ad injection.
- ▶ Consider reducing buys for older browsers.
- ▶ Announce your anti-fraud policy to all external partners.
- ▶ Budget for security.
- ▶ Continuously monitor sourced traffic.
- ▶ Protect yourself from content theft and ad injection.
- ▶ Consider allowing third-party traffic assessment tools.

— M.J.M.