THE 614 GROUP

2017 State of Digital Publishers' Fight Against NHT: To Block NHT or Not to Block?

A Research Piece by The 614 Group

Underwritten by
Distil Networks supported by Digital Content Next

614
GROUP

2017 State of Digital Publishers' Fight Against NHT: To Block NHT or Not to Block

ACKNOWLEDGMENTS

We would like to thank the following people for their insights.

Andrew Cisek, CEO; Real Good Media

Dennis Colon, VP of Ad Operations & Strategy; CBS Interactive

Jason DeMarco, Vice President, Programmatic & Audience Solutions; A+E Networks

Charles Eggleston, Vice President, Advertising Operations; AccuWeather

Dr. Augustine Fou, Cybersecurity and Ad Fraud Researcher; Marketing Science Consulting Group, Inc.

Matt Katz, Senior Director Ad Operations/Sales Operations; Univision Communications Inc.

Lisa Kerr, SVP, Market Development; Digital Content Next

Adam Moser, Head of Ad Operations; Hulu

Lois Nix, Senior Vice President, COO Advertising Sales; The Weather Company

Steven Suthiana, Global Head, Digital and Media Operations; Fast Company and Inc. Media

Mitchell Weinstein, SVP, Director of Ad Operations; IPG Mediabrands

TABLE OF CONTENTS

Executive Summary
Background/Methodology 3

What We Learned 5

Interview One: An Advertiser's Perspective 11

– Interview with Mitch Weinstein, Head of Ad Operations, IPG Mediabrands 11

Interview Two: A Brand Perspective 18

– Interview with Adam Moser, Head of Ad Operations, Hulu 18

Critical Insights 22

Conclusion 25

614 GROUP

The 614 Group

Executive Summary

Background: Are Publishers and Advertisers on the Same Page?

According to the IAB, digital fraud costs advertisers $8.2 billion each year. Some suspect there's little incentive to fight it,[1] as so many players benefit from it in one way or another. Some even suspect that publishers have a hand at it, as bot traffic is often a result of purchasing traffic. Others, including notable security expert Dr. Augustine Fou say that fraud is inevitable, since there will always be "hackers who are very advanced in the use of technology and who don't play by the normal rules of engagement."[2] If the $8.2 billion sum is correct, fraudsters are highly motivated to ensure their lucrative businesses succeed.

To date, the dominant approach to addressing fraud has been largely **reactive**: a reputable third-party measurement company, or even an agency, audits a publisher's traffic and, if fraud is detected, **reports on the percentage** that is non-human traffic (NHT)

To date, the dominant approach to addressing fraud has been largely reactive: a reputable third-party measurement company, or even an agency, audits a publisher's traffic and if fraud is detected, reports on the percentage that is non-human traffic (NHT). If that percentage is unacceptably high, advertisers are free to block that publisher or sources of media from future campaigns or simply not pay for NHT the traffic.

The reactive approach accepts fraud as inevitable; a scourge the industry must learn to live with. But is it? To find out, we designed a quantitative and qualitative survey that probed specific questions, such as:

- Are sellers of media (aka "publishers") perpetrators or victims of fraud?[3]
- If acquiring traffic is a legitimate business tactic for building an audience, what can be done to make this practice safer?
- Is a reactive approach to fraud (i.e. auditing traffic reports post fraud detection) really the best way to tackle the issue?
- What redress do publishers have when accused of fraud, either by an advertiser or by a third-party measurement company?
- What is the ROI of taking an aggressive approach to fraud?
- Can that $8.2 estimate amount of NHT in the market be isolated into a per site amount and a per campaign amount so that relevant investment decisions can be made to tackle it?

1 http://adage.com/article/digital/online-ad-fraud/292285/

2 hackers who are very advanced in the use of technology AND who don't play by the normal rules of engagement.

3 http://adage.com/article/digitalnext/real-victims-ad-fraud-surprise/296941/

614 GROUP

Methodology

We sought to answer key questions using a variety of methodologies:

Questions Raised	Methodology
What are the attitudes and perceptions publishers hold with regards to the myth and reality of fraud prevention?	Mass-market survey of 40 of the largest 250 media companies in the US including AccuWeather, A&E Networks, Hulu, Thomson Reuters and Univision.
How do industry leaders on the buy-side think about the findings of the research? How do buy-side industry leaders feel about the current state of fraud prevention, what are their current expectations?	The 614 Group conducted one-on-one interviews; one with the buy-side and one with the sell-side. Then, they hosted round table discussions with industry leaders to discuss the findings.
As a followup to this research, The 614 Group is currently seeking partners for a sophisticated testing program to close the gap between the hypothetical and the specific.	The test we are contemplating reviews the effects of advertiser, publishers and overall user experiences in an environment with and without (blocked NHT). The results will consider the related KPIs with and without the existence of NHT on a particular campaign and media company.

614 GROUP

What We Learned

- Most publishers **(78%)** are victims of NHT; yet only **38.4%** purchase traffic. Clearly, NHT is getting onto their sites through other means, which is of no fault to the publisher. For this reason, many marketers are losing trust in the digital advertising marketplace.
- Spurred on by the Association of National Advertisers (ANA), marketers are no longer willing to pay for NHT. **74%** of publishers said that traffic quality issues are part of pre-sales discussions, and 68% said they've received RFPs that included acceptable NHT thresholds. There is significant profit in fraud (IAB estimates that fraudsters siphon $8.2 billion each year from advertisers) — a figure that is an irresistible incentive for determined and skilled fraudsters to engage in these practices [4].
- The cost of fraud is greater than the NHT that arrives on a publisher's site. It should also include the ad units purchased by advertisers in the open ad exchanges -- ad spend that should and would have gone to them. If publishers were to calculate their total losses, they would realize ***their share*** of the $8.2 billion lost to fraudsters each year is much higher than previously realized.
- Publishers must draw a connection between the $8.2 billion lost to fraud and campaign-level damage. Publishers see the cost of fraud as the revenue lost when post-campaign traffic is assessed, and the traffic that's identified as NHT is compensated. Advertisers have a much different view. To them, NHT is an $8.2 billion crime perpetrated against them each year, and they are increasingly wary of the digital channel as a result. To them, publishers need to take the total cost of fraud more seriously.
- Based on the survey results and interviews, it is very clear that neither by buy nor sell-side are tracking or assessing the impact of NHT on the campaign level, which is why there is the huge disparity between publishers and advertisers. As noted above, the true cost of fraud on the campaign level is far higher than the bots that arrive on the publisher's site; it's also the fraudulent traffic sold via the exchanges. And while almost 70% of publishers believe that it's possible to calculate sold via the open ad exchanges and networks the ROI of effective anti-NHT efforts on a per-campaign and per-client basis, none of them are yet doing so.
- The ultimate solution, therefore, is to proactive block NHT traffic before it arrives on the publisher's website. Doing so will prevent the fraudsters from creating fraudulent look-alike users that are then sold on the exchange. Ironically, 70% of publisher believe it's possible to proactively block NHT, yet less than one-third of the publishers take that approach. We believe that if publishers had true insight into the total cost fraud -- to the publisher, their clients, and the industry as a whole -- the gap between publishers w publishers would take steps to proactively block fraud.

[4] https://www.iab.com/news/digital-ad-industry-will-gain-8-2-billion-by-eliminating-fraud-and-flaws-in-internet-supply-chain-iab-ey-study-shows/

614 GROUP

Leveraging online and offline research methodologies, the team at The 614 Group spoke to 40 of the world's largest media companies based in the United States.

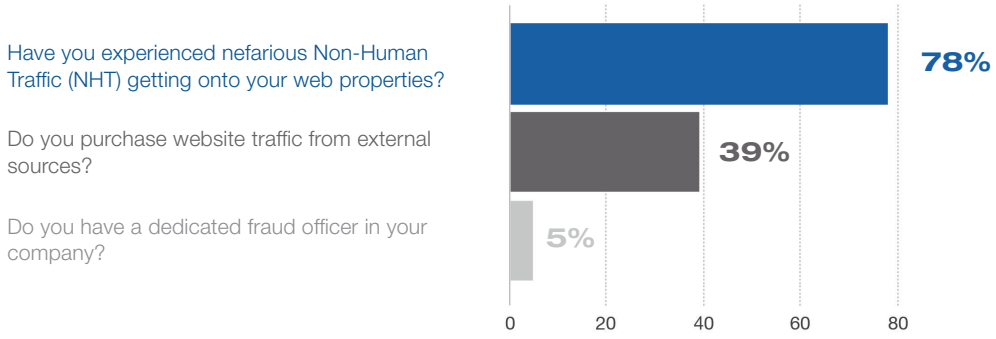
Leveraging online and offline research methodologies, the team at The 614 Group spoke to 40 of the world's largest media companies based in the United States. The surveys were completed over the six week period of October 1st 2016 through November 15th 2016. Participants included representative companies such as AccuWeather, Fox Entertainment and Television, Thomson Reuters, and Univision.

How Widespread is Fraud?

How pervasive is non-human traffic (NHT)? It's a problem that affects a wide swath of publishers **(78%)**. And while it's common to place fault on buying traffic, most publishers don't engage in that tactic. The continued attention to this means the industry still doesn't know exactly how NHT traffic makes its way to publisher sites.

- **78%** of publishers report experiencing nefarious traffic on their sites
- But only **39%** say they actually purchase traffic

Fraud by the Numbers



Response to Fraud

A scant **5%** of publishers have a dedicated fraud officer in their company, yet **78%** of publishers have battled the issue. This may be an indication that at the present moment, publishers don't see fraud as a mission-critical issue, or at least have yet to register a significant impact of fraud to their sites or their brands.

The lack of a dedicated resource may change now that advertisers are beginning to engage third-party measurement companies to track fraud, and many (see below) are including anti-fraud requirements in their RFPs.

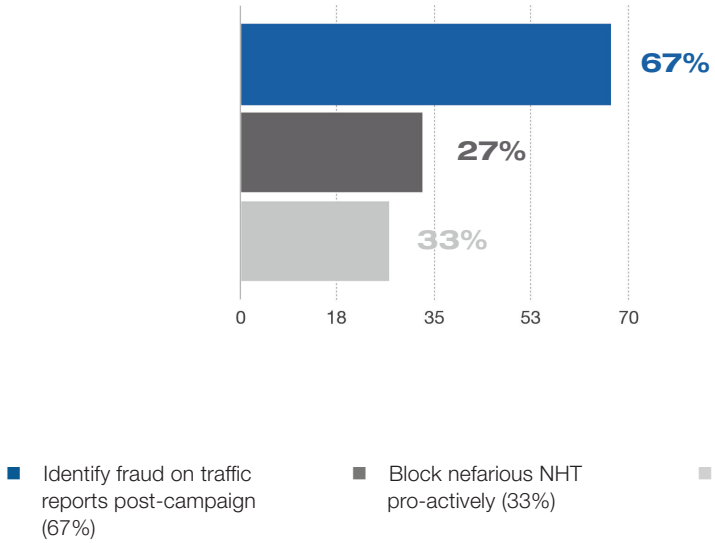
614 GROUP

Approaches to Combatting Fraud: Blocking v. Auditing

Post-traffic audits are the most common response to fraud (66.67%); and only half as many publishers (33%) make an effort to block NHT traffic prior to it reaching their sites.

- **67%** identify fraud on traffic reports post-campaign
- **33%** block nefarious NHT proactively
- **27%** both block and audit

What approaches do you use to combat fraud?

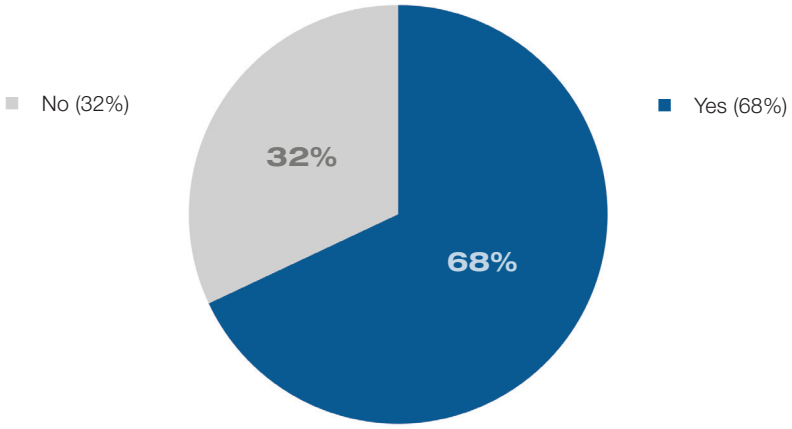


Is it Possible to Proactively Block Fraud?

We asked publishers if they felt it was possible to stop fraud from reaching their site, and **68%** believed that is was. This is an interesting finding, given that, as noted above, only **33%** of publishers use proactive fraud-blocking technology on their sites.

614 GROUP

Is it possible to stop fraud from reaching your site?



Advertiser Attitudes towards Fraud

Advertisers understand that nefarious NHT is a difficult scourge to conquer. That said, they're beginning to exert pressure. Some 74% of publishers say that traffic quality is a discussion topic in the pre-sales agreement, which means publishers need ready answers at their disposal.

- **74%** of publishers say that traffic quality is a discussion topic in the pre-sales process

Current State of the Market: Advertisers Who Name an Acceptable Level of NHT Fraud

Of the respondents who said that an agency buyer has specified an acceptable threshold of fraud in an RFP, **68%** said the threshold was in the range 2% - 5%.

The question of acceptable NHT thresholds will certainly give rise to contentious discussions in the not-too-distant future. *The ANA, as Mitch Weinstein pointed out, now recommends that advertisers refuse to pay for NHT.* And publishers that experience 10% or more NHT may be asked to defend their traffic.

Current State of the Market: Receiving Notice of Fraud/Blocked Due to Fraud

How often are publishers asked to defend their traffic? How many have been blocked? At present, notices and blocking don't appear to be major issues: Only **17%** of publishers to date have received notice from an advertiser regarding high levels of fraud. And most publishers **(86%)** have not been blocked due to fraud.

Only **17.41%** of publishers to date have received notice from an advertiser regarding high levels of fraud. And most publishers **(85.72%)** have not been blocked due to fraud.

Going forward we expect this to change, as more advertisers engage third-party measurement companies to track fraud levels, and as the ANA encourages its members to get tough on fraud.

- **11%** of publishers received notice of fraud from a buyer
- **9%** have been blocked by an advertiser, ad exchange or ad network
- **6%** have both been blocked and received notice
- **71%** have never received notice or been blocked
- **3%** of publishers responded "don't know"

Getting to the Bottom of Fraud Charges

What happens when advertisers say that a publisher has exceeded its acceptable fraud thresholds? Are these easy issues to resolve? These are urgent questions, as being blocked by an ad exchange, for instance, can result in severe reductions in revenue.

Of those publishers who experienced a notice:

- **56%** found the process of resolving it onerous and time consuming
- **44%** said it was relatively or moderately easy to sort out
- **33%** of publishers who've received notice or have been blocked said they lacked the tools to defend their traffic

Inadequate Third-Party Audits

80% of publishers report a lack of insight into how their traffic is audited by third-party measurement companies. Almost **86%** of pubs have not been blocked due to fraud universally **(80%)**, publishers report a lack of insight into how their traffic is audited by third-party measurement companies. This contrasts with Mitch Weinstein, who said his firm shares the information with publishers. The source of this disconnect would be worth exploring in future surveys, and eventually the industry may need to define a set of standards for auditing traffic.

Calculating ROI on Fraud-Free Traffic

Ensuring NHT-free traffic may require publishers to allocate time, budget and may need additional headcount to the activity. If publishers can calculate the ROI of such activities, they could more easily justify the expense. But that begs the question: Is it even possible to calculate the impact of effective anti-fraud activities on a per-campaign or a per-client basis? Sixty-nine percent of publishers **(69%)** say that it is possible to calculate that ROI.

614 GROUP

Charging a Premium on NHT-Free Traffic

Should advertisers pay a premium for traffic that has been certified delivered to real humans? Can publishers justify additional costs for their efforts? 65% of publishers say yes.

- **65%** of publishers believe that a premium for certified NHT-free traffic is justifiable.

614 GROUP

Interview One: An Advertiser's Perspective

Digital advertising couldn't exist without the active participation of agencies and marketers who invest their media spend into the digital channels. As part of our research for this report, we interviewed Mitch Weinstein, SVP, Director of Ad Operations at IPG Mediabrands regarding NHT, and the best strategies for eliminating it.

Mitch Weinstein oversees the US team of Ad Operations professionals at UM, Initiative, BPN, Cadreon and Reprise. He and his team focus on the latest in ad serving, targeting, and measurement technologies, ensuring that clients are making the most of their media budgets, reaching their target audiences, and achieving their business objectives in the most efficient manner possible.

Prior to joining IPG Mediabrands in 2008, Mitch was the Director of Sales Planning and Operations at Revolution Health Group, later purchased by Everyday Health, where he was responsible for inventory management, proposal development, revenue analysis, and ad operations. Before Revolution Health, Mitch worked for BabyCenter, a division of Johnson & Johnson for over 4 years in planning and operations.

What are the current market opinions in combating fraud capabilities, specifically blocking non-human traffic (NHT) vs. post-detection auditing?
The ideal is to block ads from serving into fraudulent environments. There are different opinions about blocking. Some people feel it has the potential to tip off the fraudsters, enabling them to determine what's being detected in order to reverse-engineer their technology and get around the blocking. But overall, I think the ability to block your ads from serving into fraudulent environments is very beneficial, because it means your clients aren't paying for impressions served fraudulently, which is ultimately the goal.

But overall, I think the ability to block your ads from serving into fraudulent environments is very beneficial, because it means your clients aren't paying for impressions served fraudulently, which is ultimately the goal.

We're trying to get to a point where clients and agencies don't pay for impressions that are non-viewable or served fraudulently. The standard way of addressing fraud — serving into fraudulent environments followed by a back-end analysis and make goods — isn't going to get us there. It doesn't really protect the client's investment in terms of only paying for impressions that are fraudulent free.

What are today's realities in terms of the ability to proactively block fraud? Is it in line with your expectations? Do you think publishers can do what they would like to do?

That depends on the vendor or expert you talk to. We've done tests with overlapping vendors and there definitely is a benefit to blocking the ads from serving into fraudulent websites. We've seen very low fraud rates from most of our media partners (which, by the way, have been confirmed by external partners).

So do I think we can get to a perfect technology that always blocks 100% of fraud proactively? Of course not, we're likely to encounter some level of fraud as long as there is money to be made and there are smart people out there creating bots. But we can keep it to a low, single-digit percentage, level and then optimize out of those areas. I think that right now, those are the best tools we have.

There are tools we can leverage, but there's also vigilance. Just paying attention to the data, looking at it on a regular basis, talking to media partners, and vendors on what it means, and how fraud is measured and detected...these conversations are some of the best tools we have right now.

What data do you look for when seeking to assess the power of blocking?

Verification data is the foundation of our efforts. For instance, we want to ensure that our viewability-verification vendor is filtering out fraud, so that fraudulent impressions, which can look viewable, are removed from those counts. We want to make sure that all traffic is filtered based on the sophisticated invalid-traffic guidelines, not just the general invalid-traffic guidelines. We pay close attention to data that tells us the number of impressions, blocks, fraud detected, viewable impressions based on different standards, time and view, things like that. Our media planners and buyers look at that data, and use it to optimize, pay bills and reconcile invoices.

Additionally, when we buy programmatically, we almost always use pre-bid technology, which means we look at the ability to block impressions before we even make a bid on an impression. We also look at the discrepancies between that pre-bid ability and the post-bid technology. Overall, we look at performance, correlating fraudulent percentages and environments to overall media performance, to assess the impact of fraud. I think this is most critical because ultimately that's what we're after — efficient media performance. Eliminating fraud is a way to get there. Reduction in fraud is not necessarily a KPI, it's just a way to make media perform better, and it does correlate to better performance.

Overall, we look at performance, correlating fraudulent percentages and environments to overall media performance, to assess the impact of fraud. I think this is most critical because ultimately that's what we're after — efficient media performance.

614 GROUP

Have you identified any specific performance KPI's that are particularly indicative of bad traffic?

No, I haven't seen anything that specific. Each client will have different KPI's; some measure in-store purchases, others focus on online conversion or online sales. This is hard it hard to identify the exact KPI's that are associated with low fraud. That's why the overall goal is to draw the correlation between brand safe, low fraud and higher performance.

This is hard it hard to identify the exact KPI's that are associated with low fraud. That's why the overall goal is to draw the correlation between brand safe, low fraud and higher performance.

Many people in the industry feel publishers aren't innocent players, believing that bots are almost ushered onto sites when publishers acquiring traffic, or when they lack a mechanism to identify and block bots. This, by their definition, makes the publisher complicit in fraud. Do you agree?

No, I think most of the publishers, at least the ones we work with, do everything they can to prevent bots from their sites. Again, it's not 100%, but they know we're watching and tracking, so there's no benefit to selling media that's highly fraudulent because we will catch it.

There are other publishers out there on the long tail who buy traffic from sources that aren't of the highest standards. In such cases, you may find a lot of fraud and bot activity. But we don't see that very much with the publishers we work with directly.

"I think most of the publishers, at least the ones we work with, do everything they can to prevent bots from their sites."

Our survey found that 77.5% of publishers have seen NHT hit their sites, but only over 63.2% say they purchase external traffic. How does it get onto sites?

The bots are smart. They're trained to go to numerous sites and get tagged with cookies so they look like a real consumer. They may go to ESPN.com to look like a sports fan, and then check email somewhere. They'll bounce around to get tagged at various sites, and visit a high-end automotive site so they're tagged as an auto-intender and become attractive to automotive media buyers. These bots don't just sit on low rent, unlit sites; they're programmed to visit a lot of premium sites so they'll look like targetable humans. And that's the fraudster's goal: To create bots that are ultimately targeted with the most premium quality media, especially video. Given this, I don't think that a site is complicit, as long as they're doing everything they can to keep bot levels low. But it's really hard to block it all.

614 GROUP

What do you think of the practice of audience buying in general? Do you have an opinion on it?

I think it's okay as long as the publisher fully discloses that additional media will be purchased on properties that they don't own and operate. But again, we need to protect our investment with some kind of verification service so we can easily and quickly detect if that audience-extension program is leading to a lot of fraud. Publishers know when and what we use in terms of verification, so they're usually pretty smart about it. As a result, the quality of their audience extensions is usually pretty good.

From our survey we learned that for the last year or so, publishers have been handed a NHT threshold in RFPs, and that threshold typically falls between 2% - 5% as an acceptable limit. While no amount of fraud is acceptable, can you explain why a threshold like this may make sense?

It's not necessarily a threshold, it's just putting a cap on what's acceptable to buyers in terms of of fraudulent impressions they buy. Buyers understand that despite best efforts, some bots will always get through. They don't want to pay for it, but they also don't want to "punish" the publisher by saying "we're not buying from you anymore." That's not what the threshold is about. The threshold could be whatever you want it to be, say 25% or 50%. But if a buyer says, "whatever comes back as fraudulent, I'm not paying for," that's more important than accepting a certain level of fraudulent impressions.

I think for a publisher with a 2-3% bot traffic is okay because then they know it's not really going to affect their overall revenue. They might need to make some adjustments in terms of what they charge on a media CPM-basis, but overall, a small single-digit percentage of bot traffic won't have a huge impact on their overall revenue. But if their fraudulent rates are very high and buyers say they won't pay for that, then they're on the hook for losing a lot of inventory that they can't sell.

It's not a case of buyers saying, "you have 5% fraud we're not going to buy from you", It's more a matter of: If we serve 100 impressions and 5 of them are served to a bot, we'll only pay for 95. That's also coming from Association of National Advertisers (ANA) and from our clients."

It's not a case of buyers saying, "you have 5% fraud we're not going to buy from you." It's more a matter of: If we serve 100 impressions and 5 of them are served to a bot, we'll only pay for 95. That's also coming from Association of National Advertisers (ANA) and from our clients. There's a big demand right now to make sure buyers don't pay for non-viewable or fraudulent impressions. In many cases this is being done already, and it isn't groundbreaking. Most agencies do this to some extent already. But I think it's going to make it more official and more ubiquitous.

Regarding notification of NHT, how do you determine if a publisher has given you that bad traffic?

It's in the reporting from the verification companies, and our teams look at that data on a regular basis so they can see, pretty easily, breakouts by media partner, campaign and site, and the different levels of fraud and non-viewable impressions. Once detected, they can have a conversation directly with the media partner, especially if the rate of fraud is higher than all the other media partners.

Additionally, we share that data directly with anybody from whom we buy media so that they can access the verification report and monitor and manage it themselves. We strongly encourage this among our media partners, as it's essential to be vigilant on all angles.

From our survey we learned that publishers overwhelming feel they don't have enough insight into why and how their traffic was being measured. Why is that, in your opinion?

Probably because there isn't an effective communication plan between the media buyer and the media owner. That's really what it comes down to. For our process, we include in the RFP exactly what we're measuring against; exact goals in terms of the viewability rate; whether we're at a point where we are only paying for viewable impressions vs non viewable; and if there is a percentage goal of viewable impressions.

All of these expectations are included in the RFP. And in the I/O it will state the measurement partner we use, and that we will provide access to the data from the measurement partner. All publishers should get this level of data, and make it a part of any standard proposal. As part of the proposal back to any RFP, they should ask for that information.

"Probably because there isn't an effective communication plan between the media buyer and the media owner. That's really what it comes down to. For our process, we include in the RFP exactly what we're measuring against"

614 GROUP

Even if buyers don't ask in the RFP, publishers should still ask: what's the viewability expectation, what's the fraud expectation, what are you measuring, which vendor are you using, how often are you looking at the data, can we access directly to that data? If publishers are in the dark, they won't get the data they need to optimize, and they will be held to unknown standards. That's not good for anyone. So whether it's an agency failing to provide adequate information, or a publisher not asking the right questions, there's still a breakdown somewhere that impacts the publisher.

What are the right questions to ask if a publisher is notified of high levels of NHT?

- Is there a viewability goal?
- Which vendor are you using to measure viewability?
- How can I access to the data from that vendor?
- How often will you optimize?
- What are your overall expectations?

A major goal for industry is to diminish NHT, but with the understanding that fighting the problem costs money. Has your team been able to measure ROI on media buys with and without NHT?
We're working with some vendors that have deeper analytics around ROI, and we can now distinguish and measure causal impact versus an event that would have happened even if that person had not been exposed to media. So again, it's a matter of contrasting the two, and ultimately determining the overall conversions and metrics to assess the impact of blocking fraud on driving key performance metrics. That's really getting into a deeper set of analytics, and that's definitely something that we're working towards, and we have some teams looking at all this data. So it's hard for me to say exactly how all that would look right now.

Can you measure this down to the campaign level? For example, can a J&J campaign clearly perform better with 2% NHT vs 7% NHT? And if yes, have you shared this data so a publisher can make the proper investments to stop it?
That's how we would look at it. Because going overall campaign-by-campaign would have different metrics and different goals. So we would look at in the campaign level.

Do you think this is a good idea?
Definitely. That's the key, right? The whole point is to get better quality media so it performs better. It's a deep analysis, and cost is an essential part of it. If there's an increased cost and a better quality, is it worth it? Is it driving metrics more efficiently when you factor in cost versus paying a cheaper rate for media that's not as high quality. You're getting more media, but a lot of it might be fraud or non viewable. So ultimately it varies.

But the goal should always be to make sure your media is more effective.

What does the future of combating fraud and NHT look like? What's the forecast for dealing with NHT issue? Will it get easier, harder, or stay the same into the next 12 months?

More and more advertisers will include in any I/O or contract with the publisher stringent fraud terms. They'll say they won't pay for impressions that are fraudulent. That could be bot, or it could be bad behavior by a publisher. Whatever it is, and whatever is caught by the verification provider, will not be paid for by the marketer or the media buyer.

This is already happening in a lot of cases, but I think more clients are pushing on this, and it's becoming more official with ANA. The ANA is including this in there standard guidelines to their members, and it's going to continue to roll through the supply chain. This will be a significant development in the coming year. It will become a standard requirement, even with media buyers who aren't currently transacting this way today. It will become an essential requirement for quality.

I think clients will increasingly understand that to get better quality inventory, and consequently better performance, additional costs are necessary. I think that's going to be important. Those bottoms of the barrel rates you get with open exchange programmatic come with a separate price which is not always the highest quality inventory. So I think more and more media buyers will understand that and will focus on that.

Interview Two: A Brand Perspective

To gain a publisher perspective we we interviewed Adam Moser, who leads Hulu's Advertising Operations where he is responsible for driving forward Hulu's efforts to deliver best-in-class advertising across Hulu's desktop, mobile, over-the-top, and other emerging premium video platforms. Prior to joining Hulu, Moser was the Vice President of Digital Sales Operations at NBC Universal where he oversaw the ad operations teams responsible for executing across the company's broadcast and cable portfolio. In preceding roles, he was part of Sales Operations at CBS Interactive managing video ad implementation across CBS Sports and Entertainment as well as at MTV Networks helping to establish and execute ad serving on Viacom's first foray into their online full-episode streaming.

In general, do you think blocking NHT is possible? Have you thought about the idea of blocking it?

Yes, blocking NHT is possible. There are a handful of companies in the industry that have developed some interesting solutions for publishers to do so. Some will aim to block these fraudulent impressions outright, while others will count and isolate NH-served impressions.

Hulu has its own ad server and proprietary technology, and we also examine and filter out this type of traffic.

I think part of the responsibility to identify NHT lies with the ad servers themselves. Hulu has its own ad server and proprietary technology, and we also examine and filter out this type of traffic. Given that we bill on completed impressions instead of starts, our advertisers are never charged for any impression that hasn't been fully viewed by a human.

Do you think that certified non-NHT (certified human traffic) should be priced higher in the marketplace?

I'd like to think most publishers can say their traffic is priced on the principle of delivering human-viewed impressions, but we know that's not always the case, even if unintentional. To a degree, viewability-as-a-currency set a precedent, with agencies requiring a guaranteed viewable return, and costs associated with third parties validating that traffic for both sides entering the negotiation.

To a degree, viewability-as-a-currency set a precedent, with agencies requiring a guaranteed viewable return, and costs associated with third parties validating that traffic for both sides entering the negotiation.

614 GROUP

What does the term "Human Viewable Impression" mean to you?
It's about advancing the definition of the viewability metric beyond the filtration of NHT. Agencies and marketers are increasingly concerned with ensuring their media dollars are not only viewable by our industry's standards, but certified as served to human eyeballs as well, removing any doubt of paying for a fraudulently-served impression. Third parties have already taken steps to fold this type of data into their analytics so that human and viewable impressions can become their own metric. Ultimately, the fact that the industry had to create this term displays that we still have a trust issue with marketers.

Ultimately, the fact that the industry had to create this term displays that we still have a trust issue with marketers.

Has Hulu ever received notice from a buyer that they have found NHT somewhere? If yes, did you get adequate data to help you understand why your traffic was deemed NHT?
We work with a number of third-party partners that report NHT and we consistently find that less than 1% of impressions fall into this category.

That said, there is still a need for further education within the industry to understand why and how impressions may be categorized in this manner, particularly as the amount of third parties measuring this data continues to fragment. We have seen this as these partners re-affirm their methodologies to the buy and sell sides when discussing this type of traffic, as the focus on viewable and human impressions blend into a unified metric.

Have you ever looked at calculating the effects of NHT at a campaign level?
No, we haven't taken that approach because our extraordinarily low amount of NHT speaks for itself. We will support any advertiser who wants to work with one of our partners to measure this for their campaign's directional purposes, because we stand behind our numbers. In addition, we also look at it in aggregate for our ad server which aligns with what we see at the campaign level.

We will support any advertiser who wants to work with one of our partners to measure this for their campaign's directional purposes, because we stand behind our numbers.

614 GROUP

From our survey we have learned that for the last year or so, publishers have been getting a NHT threshold given to them in an RFP and it's been between 2% - 5% as an acceptable limit. Do you think that is a reasonable number for the marketplace? Not Hulu specific.

That matches what we've heard. We have to be careful as an industry though. Just like with any third-party measured impression, you're going to have some level of discrepancy. The more partners that measure NHT with differing methodologies, the more those discrepancies may vary over time, and the value of human vs. non-human gets muddied.

The more partners that measure NHT with differing methodologies, the more those discrepancies may vary over time, and the value of human vs. non-human gets muddied.

There is an argument out there that says, even if it's 1% or 2%, that actual impact is much greater because when people are grabbing these cookies, they take the cookies and they place this information on exchanges and they resell traffic that looks and feels like Hulu users to people who would normally want to buy Hulu. So that's a revenue loss that should be going to you but is actually going to a fraudster. React to that. Do you ever think about that and the impact 1% or 2% could have?

This isn't a concern for us because the majority of our traffic comes from non-PC, non-cookie-based devices – in fact, less than 10% of our traffic is via PC. Additionally, our Advanced TV offering is **private**, so it would be a red flag for us if we were to find out that Hulu traffic was being resold.

Some advertisers are considering reallocating budget away from digital until the fraud issue is resolved. Is this something your clients have raised?

Understandably recent headlines have caused some unease in the marketplace, but no, we haven't experienced this. Hulu is an advertiser-friendly, safe environment, with Jack Meyers and MyersBizNet rating Hulu as the #1 safest site for advertisers. We bill on completes, we have a 92% video viewability rate, and NHT is a non-factor. Fraud is not an issue our advertisers have to worry about.

Hulu is an advertiser-friendly, safe environment, with Jack Meyers and MyersBizNet rating Hulu as the #1 safest site for advertisers.

Why do you think there is such a gap in understanding the presence of NHT? Why such extreme language on one side?
I think there's such extreme language on one side because not every publisher has less than 1% NHT. If you're on the buy side and are seeing significant numbers, you should question why it's so high. To me, the non-human conversation in 2016 is what the viewability conversation was in 2012.

To me, the non-human conversation in 2016 is what the viewability conversation was in 2012.

Technology will help shape the standards that will yield better returns for our advertisers. Today, the technology exists to determine whether an impression was viewable and coming from a human or fraudulent source. While the methodologies may improve over time, ultimately, if you're a publisher and not willing to work with one of the vendors in the space that can measure this type of traffic, my question is, what are you hiding?

Has your team measured ROI on media buys with and without NHT?
No, because Hulu has extremely low NHT, measuring ROI on media buys with and without NHT doesn't uncover measurable ROI difference for our advertisers. Like TV, there's not much NHT to measure against. That said, our aggregate ROI is high across all campaigns, with Nielsen Brand Effect data showing that ads on Hulu are, on average, 20% more effective than on TV.

Do you guys have a dedicated compliance officer or traffic officer at the company?
We do not. We do, however, work with over a dozen measurement companies to help marketers confidently transact with Hulu.

Most publisher do not have one. 90% of publishers do not.
Publishers can't get away with grading their own homework, so third-parties will continue to have a space to measure for fraudulent activity. That said, this will be interesting to see if these roles are established more commonly as publisher's site strategies evolve over time to combat this challenge.

Critical Insights

At the November 2016 Brand Safety Summit presented by 614 Group, we heard marketers say they are losing trust in digital advertising and if NHT isn't brought under control soon, they will consider cutting digital budgets and re-direct their spending. At the November 2016 614 Group Brand Safety Summit, we heard marketers say they are losing trust in digital advertising and if NHT isn't brought under control soon, they will consider reallocating their digital budgets to traditional channels that offer guaranteed brand safety.

All publishers are victims of NHT, but it can't be all their fault

78% of premium publishers surveyed report experiencing nefarious NHT on their sites. Across the industry (as noted above), there is a perception that NHT is a direct result of engaging in questionable tactics, such as purchasing traffic to increase their volume. But only 38.4 % of the respondents say their sites actually purchase external traffic. Clearly NHT is hitting on most publishing sites despite publishers following current best practices which means Marketers will continue to lose trust in the marketplace unless publishers improve on the current reactive tactics.

Clearly, NHT is finding its way on to sites via other means this represents an example of why Marketers are claiming to have lost trust in the marketplace.

But advertisers are increasingly frustrated with NHT, as $8.2 billion is an alarming amount of money to lose. Adding to their frustration, they pay a host of monitoring, measurement and brand-safety vendors to ensure their ads are seen by real humans in brand-safe environments. In spite of these investments, fraud continues to escalate.

Differing attitudes regarding the cost of fraud

One of the more alarming conclusions is the disparity in publisher and advertiser attitudes towards the inevitability of fraud. At present, monitoring fraud is the preferred method for addressing NHT (73% of respondents rely on this method). This approach means that publishers lose a small amount of revenue individually in each campaign, while the nefarious players collectively gain $8.2 billion. This perception in difference is critical: Publisher's view NHT as the small revenue hits they incur with each campaign, while advertisers view it as a colossal $8.2 billion crime that is perpetrated against them annually.

614 GROUP

The difference also illustrates a major gap in between buyer and seller in current market dynamics: Today, publishers are not aware of their true pro-rata share of that $8.2 billion (see below). If publishers understood the scope of their losses — and we believe that those loses are in the millions — they would certainly invest the necessary budget to fight it. The trouble is, neither publisher nor advertiser is tracking the total cost of fraud on a campaign level. That means publishers are blind to their true costs, and advertisers don't have the data they need to help publishers gain insight into the problem.

It should come as no surprise that auditing traffic post campaign is no longer sufficient. In fact, Bob Liodice, CEO of the Association of National Advertisers (ANA) threw down the gauntlet, telling the ANA members, "Ad fraud awareness has improved but effective action is rare. You shouldn't be paying for this."

This attitude is increasingly revealed in the sale process. According to our survey results, 74% of publishers report receiving RFIs that include requirements for traffic quality.

The cost of fraud is greater than the NHT that arrives on a publisher's site

The NHT impressions on publisher websites aren't the true cost of NHT penetration to publishers. Criminals aren't interested in increasing impressions on sites they can't monetize, so publishers shouldn't focus on their direct loss. Instead, publishers need to determine the actual loss of revenue based on the multiplicity of visits to a fraud site by a bot — bots that may visit their sites only once.

Put another way, let's assume that site, called "PremiumNews.Com" (aka PN.com) is a publisher that sells impressions at $2.00 CPM. When a bot visits that PN.com just once, the direct revenue loss is insignificant. But by visiting the site, that bot creates an identity of PN.Com user. That same identified user will now be sold as an ad unit on a fraudulent site 10,000 times.

Let's further assume the fraudulent site sells these impressions programmatically at $.20. The actual revenue lost by PN.com, therefore, shouldn't be determined by its sold CPM; rather, it is the $.20 paid by advertisers eager to target PN.com users, is now collected by the fraudsters, times 1,000 impressions. The loss, therefore, is a $200 CPM, 100x larger than the direct calculation. This is money that should have gone to PN.com and never did.

Publishers must draw a connection between $8.2 billion and campaign-level damage

Almost 70% of publishers believe that it's possible to calculate the ROI of effective anti-NHT efforts on a per-campaign and per-client basis. This is an important exercise, since many publishers will need to make significant investments in technology, try new approaches, and headcount (including a dedicated fraud officer or equivalent role) in order to successfully combat fraud. To justify those expenditures, many publishers need a way to to connect the dots between the $8.2 billion that's collectively lost to fraud, and the damages that occur on a campaign or client level.

70% of publishers believe proactively blocking NHT is possible

The majority of publishers (70%) surveyed said they believed it was possible to proactively block NHT from reaching their sties. If that's the case, in light of the risk NHT poses to the long-term viability of digital advertising, it's intuitive that publishers should do all they can to block — rather than merely — audit it.

614 GROUP

Conclusion

In looking at NHT in the digital advertising, we see numerous gaps. There's a gap in perception of the problem between publishers and advertisers. To publishers, it's an inevitable and unfortunate revenue hit, to advertisers, it's a colossal $8.3 billion crime committed against them each year. As we stated above, the ANA advises its members not to pay for fraud, while publishers are clamoring for more data as to how buyers determine that fraud is present.

There also is a significant gap between what publishers believe they're losing, and the losses that actually affect their bottom lines. The total cost of fraud factors higher than the number of bots they must subtract from their post-campaign traffic reports. The true cost to the publisher must include advertiser spend on fake traffic designed to look like the publisher's own users, but sold in other channels.

Finally, there is a gap between how the industry should approach fraud, and how they're actually fighting it. On the one hand, it is clear that publishers understand how proactively stopping NHT from arriving on their sites is the proper course of action, yet over 60% rely on auditing traffic and compensating advertisers after the fact. We believe that unless publishers take a proactive approach, advertisers will divert their budgets to non-digital channels, at least in the short term. On the other hand, publishers report that advertisers and agencies fail to provide adequate information regarding their traffic audits. Publishers need that insight in order to assess if and how NHT arrives on their sites. Until both sides accommodate one another's needs, fraud will continue, with devastating consequences across the industry. Conversely, a proactive approach to NHT, along with greater transparency, will go a long way in instilling confidence among advertisers and publishers alike, and in securing the future of all publishers of digital properties.

614 GROUP

Distil Networks, the global leader in bot detection and mitigation, is the only easy and accurate way to protect web applications from bad bots, API abuse, and fraud. With Distil, you automatically block 99.9% of malicious traffic without impacting legitimate users.

Distil Web Security defends websites against web scraping, brute force attacks, competitive data mining, account takeovers, online fraud, unauthorized vulnerability scans, spam, man-in-the-middle attacks, digital ad fraud, and downtime.

Distil API Security protects all types of APIs including those serving web browsers, mobile applications, and Internet of Things (IoT) connected devices. Distil API Security defends APIs against developer errors, integration bugs, automated scraping, and web and mobile hijacking.

For more information on Distil Networks, visit us at http://www.distilnetworks.com or follow @DISTIL on Twitter.

614 GROUP

614
GROUP

DECEMBER 2016