WTF

is Marketing Fraud?

HUMAN | DIGIDAY

Sophisticated bots are creeping into every element of digital marketing

Online, bots are becoming more sophisticated, in that they used to behave in noticeably robotic ways and now they're increasingly human-like. They mimic human behavior when visiting websites — clicking on ads, filling out forms and surveys. Even as marketers are under increasing pressure to focus on the metrics, conversions and data-driven tactics that drive better business results, bots enter CRM systems and data management platforms, skewing results and retargeting. They steal marketers' money and then go on to waste more ad spend.

The issue is known as marketing fraud, and it's entering every tunnel and funnel of digital marketing. However, by building strategies that ensure that they are engaging with real humans, marketers can avoid hard-earned budgets being stolen and wasted, gaining a competitive advantage by addressing marketing fraud issues they might not realize they have.

In this WTF, we explore:

- The impact sophisticated bot attacks are having on marketing campaigns — driving as much as 38 percent invalid traffic
- The definition and life cycle of marketing fraud
- How agency Innocean beat the bots
- How to identify fraud in the walled gardens of search and social

---

This guide will help marketers ensure that only authentically human outcomes — and only healthy traffic, analytics and data — are the results of their digital marketing efforts.

WTF
is marketing fraud?

Most marketers are well versed in ad fraud — fraudulent activity that uses digital advertising networks to benefit financially from ad transactions — and the ad industry is actively addressing the problem. More ad fraud will be stopped this year than will succeed, according to the fourth **"Bot Baseline Report"** from HUMAN and the Association of National Advertisers (ANA) — surveying 50 ANA members. In 2017, the study projected losses to fraud of $6.5 billion whereas the 2019 study projected losses of $5.8 billion globally. It shows an 11-percent decline in two years, at a time when digital ad spending increased by 25.4 percent between 2017 and 2019.

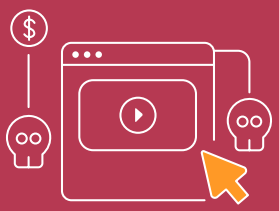
How is marketing fraud committed?

While ad fraud compromises the validity of an initial impression and whether that impression is served by a human, marketing fraud compromises the entire life cycle of every digital marketing tactic — impacting customer lifetime value and resulting in loss of revenue.

The impact to lifetime value generated from digital marketing efforts is several multiples — an estimated three-times the investment is typically lost. And the full impact of bots is not fully understood by advertisers — for example, an 8-percent loss of budget can mean revenue loss amounting to potentially 24 percent of their advertising budget. Since the loss goes undetected, the vanished revenue is irretrievable. It also means that competitors stand to gain from this lost opportunity, as real consumers are converted by someone else.

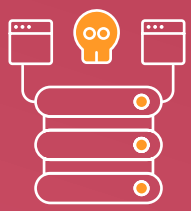
Marketing fraud

Shortlist: Threats to performance marketing

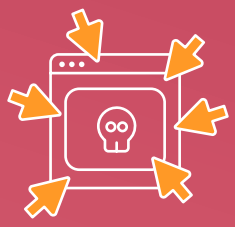


Click Fraud
Sophisticated bots get paid to view and click on ads, and the marketer is none the wiser given their human-like tendencies.

Lead Fraud
Fraudsters drive bot traffic to landing pages, typically with form fills, and emulate human behaviors to avert detection. When companies pay for leads, sometimes third-parties are tapped to meet expectations. Bots are then deployed and paid to fill out the form.



Retargeting Deception
This fraud occurs when service providers have driven site traffic from sophisticated bots which then populate DMPs or CRM systems. Fraudsters use this data to retarget bots, falsely claiming the referral payments while marketers waste time and money retargeting these bots with ads.



Competitive Assaults
"Black hat" marketers invoke click-bots to launch automated search queries, click on competitor ads to waste competitor budgets, and diffuse targeted marketing efforts.

Who is committing marketing fraud and why?

There are four main groups and reasons driving marketing fraud, today:

1. **Organized criminals and advertising intermediaries who have found a way to get paid on a CPM, CPC or CPL basis for fake/automated activity.**

2. **Black-hat marketers who waste competitors' budgets and confound their optimization strategies in order to get a competitive advantage.**

3. **Apps or software, created to collect the payout from ads, using bots.**

4. **Rogue publishers seeking to artificially inflate their traffic and make it attractive to automated targeting systems.**

The handiwork of these four groups can go unnoticed by basic analytics and brand-safety tools — but also by even the most sophisticated and experienced marketers. Whatever the skills and sophistication, there is a core step that marketers can take to stop marketing fraud, and that's to learn its life cycle — setting the stage to disrupt it and stop the loss.

The life cycle of marketing fraud

Marketing fraud touches all parts of digital marketing. Bots steal and waste marketers' ad spend on lead generation, display, native and video advertising, organic traffic, social and search. In turn that impacts the organization's tech stack, including elements of data management, CRM, personalization and marketing automation.

Fraud can manifest in any number of tactics, and when it's noticed it is often in the form of marketers saying, **"something is happening that doesn't seem human on my site."** But only if they have the proper bot mitigation tools in place to catch the increasingly sophisticated activity. While some may be able to identify a particular spike in conversions or an entry point, to avoid further wasted spend marketers need to look even deeper — to identify whether a bot has entered a data pool or a CRM system, for example, and to mitigate the impact of that bot across all optimizations and marketing strategies.

All these details fall along a life cycle, one like the illustration below.

Disrupting this life cycle is a day-to-day challenge, with bot creators becoming increasingly smarter and fraudulent operations becoming larger and more complex — operating like real businesses. For example, marketers may only see the last fraud event in a life cycle and may ask themselves questions such as the ones on the next page, but in isolation and not as part of a whole-cycle view.

Life cycle of marketing fraud

1. **Campaign goes live**
2. **Bots enter undetected**
3. **Bots infiltrate marketing activities**
4. **Marketers waste spend on targeting bots in next campaign**

Some of the questions that marketers ask about marketing fraud are as follows.

- How did a person's device get infected with malware? Perhaps they downloaded a fraudulent app.
- How did fraudsters acquire email addresses? Maybe they bought them on the dark web.
- Where did those email addresses come from? Possibly a data breach.

In reality, the answers are seldom so simple, and numerous elements are working together when fraudsters target marketers' ad spend.

"There is a part of me that admires the spammers and the fraudsters, as to the cleverness of what they do," says Mark Brill, senior lecturer in future media and creative innovation at Birmingham City University. As businesses think of ways to deal with the issue, the fraudsters will also find a way to counter it. Brill says: "It's this constant race between the two sides to deal with it."

To win that race and break the life cycle of marketing fraud, businesses need to take a holistic view of the entire marketing life cycle to make it harder for fraudsters to make money, only then will fraudsters avoid buying credentials or infecting devices.

One example of those efforts already making progress is the story of **3ve** (pronounced "Eve"), a global and complex family of online fraud operations designed to evade detection. 3ve was eventually dismantled by a cross-industry alliance led by HUMAN and Google — plus several other ad tech and cybersecurity companies — resulting in the indictment and arrest of its perpetrators; it was the largest botnet takedown to date.

> **[Fraud] is quite a dark world, and an ever changing world, so it is hard to keep up with.**
>
> — **Mark Brill, senior lecturer in future media and creative innovation, Birmingham City University**

Stopping fraudsters is a buy-side responsibility

Knowing that the fight against marketing fraud takes a more holistic view of the marketing life cycle and potential vulnerabilities, who is responsible for doing that, and what steps must be taken to make it happen?

Angus McLean, director of Ebiquity, a global marketing and media consultancy, says: "Complicated by the lack of regulation and legal repercussions, digital fraud is a high-yield, very low-risk way to divert budgets into fraudulent routes." And so, it's down to the buy-side to clean up advertising. As McLean says: "There is no incentive for any of the players to change the game. It has to start with the advertisers who control the budget to say this is no longer acceptable."

There is an incentive, however, for marketing departments looking to highlight their value to the businesses within which they operate: Identifying and tackling marketing fraud creates an opportunity to reach a verified audience and build real customer loyalty and lifetime value, in addition to reducing wasted ad spend.

> **If fraud feeds into your analytics, it will make you make the wrong decisions and optimize towards wasteful partners.**
>
> — **Angus McLean**
> **director, global marketing and media consultancy Ebiquity**

The outcomes of taking action against bots

By tackling fraudulent behavior in every aspect of digital marketing, marketers can maximize their existing efforts and focus their optimization efforts and strategies on reaching humans, rather than bots. By doing so, marketers can achieve the following:

Maximize ROI and spend
by ensuring marketing efforts are reaching humans by verifying interactions on site.

Unify analytics
by incorporating real-time data that checks the humanity of questionable patterns, pre-optimization.

Clean data pools
and trust that the data entering systems is human to safeguard targeting/retargeting efforts and preserve the lifetime value of consumers.

And so, with the responsibility on the advertiser's side, the next question is: how can marketers with the incentive to stop marketing fraud achieve that outcome? One recent case example, that of Innocean, highlights steps that work.

Interview: How Innocean defeated sophisticated bots

As an agency, Innocean works on campaigns where marketing leads go directly into a distribution system. While huge surges were being celebrated as successful campaigns, bot detection technology revealed a different story.

Seif Khemaissia, group director, programmatic and analytics at Innocean Worldwide Canada, says: "Somebody would have a huge surge on a day that we launched a campaign and everybody's patting themselves on the back saying, 'Hey, we did a really good campaign. We ran all of these leads.' But when those leads come in and you find out that they're all fake, then it disrupts the entire reporting system."

Khemaissia also sees bots that embed on websites, collecting information about audiences. From a privacy compliance perspective this is a huge problem. Innocean had protective measures in place, but still couldn't find the answers to their problems. Khemaissia says: "It's not enough to just have the technology in a black box, I need people to contextualize it and understand it for me so that I know what to do."

For Innocean, acting on bot detection insights eliminated wasted ad spend and no longer diluted re-targeting efforts by avoiding re-serving ads to bots. But a bigger part of the problem is the attribution aspect of marketing fraud, and the effect it has on analytics — making teams question the tactics that are going wrong and why.

Khemaissia says: "I'm challenging my team, 'What optimizations caused this?' wondering if it is a tactical shift that isn't performing very well. As soon as we implemented threat detection measures and removed all the known fraud, the results were night and day compared to when we hadn't noticed it. The tactical changes were actually performing very well, but the results were diluted."

Understanding bot behavior is key to the solution

The main characteristics of the fraud that Innocean saw was that 99 percent of it was coming from a Linux device and spending less than 00:001 seconds on the site. They also noticed the traffic usually came from a remote city in the U.S. and all of the traffic came from a desktop. The humans that visit Innocean's sites spend more than a second, across different devices, operating systems and browsers. This sparked a number of actions to defeat these bots.

Khemaissia says: "Preventative measures began with exploring the behavior of the bots and led to new measures on the site — all pages are now https and lead forms have functionality that blocks auto field populations, which happens with sophisticated bots that fill up forms. Implementing threat detection reporting in real time that triggers notifications is possible when you know the characteristics of the bot behavior."

Case Study: How a luxury automotive brand reduced fraud and increased conversions

Lead generation activities were driving 17 percent fraudulent leads, and 38 percent of sophisticated invalid traffic was originating from one specific advertising platform.

Identifying how and where bot activity is happening quickly and efficiently resulted in a 600-percent conversion rate for this luxury automotive brand in six weeks.

1. The sophisticated bot challenge

Brands use multiple digital marketing tactics and sources simultaneously — lead generation, social, search, mobile and display advertising — and marketing fraud can impact each and every one. In another example of how marketing can identify vulnerabilities and disrupt the marketing fraud life cycle, one luxury automotive brand with whom HUMAN worked wanted to drive potential customers to complete "configure and price" forms for its various models. When conversion rates dropped, the brand believed bots were on their site and needed to know which tactics were driving them there. The brand initially thought they could fix the problem with landing page optimization — this wasted time and money, however, and didn't solve the problem.

2. Pinpointing the problem

The brand suspected they had "some" bot activity, By using HUMAN bot detection technology they uncovered what turned out to be significant bot activity, and were able to pinpoint the specific campaigns, tactics and inventory sources that were delivering bot traffic. They were able to generate site traffic insights and acquire viewability into the entirety of their digital marketing activities this empowered them to stop attracting and remarketing to bots.

3. The post-optimization result

Using marketing fraud insights, the brand optimized its campaign and acquisition strategies completely eliminating certain tactics — in-app mobile, for example. It then focused its marketing efforts on humans by removing sources and tactics that drove fraudulent traffic — stopping efforts on specific platforms or inventory sources and doubling down on the clean ones.

Another benefit of the insights and the action the brand took is the removal of bot traffic from its marketing systems — i.e., from its data management platforms and attribution. Another benefit is that cleaner data drove better analysis: the brand was able to better understand customers when it wasn't clouded by bot activity.

In a matter of six weeks, all of these efforts resulted in a sizable uptick in their conversion rates and eliminated wasted spend on non-human traffic.

Further tactics: Fighting fraud within the walled gardens

Marketing fraud impacts areas beyond a marketer's line of sight. To truly tackle the bots, marketers also need visibility into threats and fraud coming from search and social.

Channels such as search and social are effectively walled gardens, but technology can provide a way in and help marketers understand which partners are the most beneficial and which channels are delivering the most healthy traffic. Search and social vendors have their own bot detection because they want to protect their advertisers, but managing marketing fraud must include broad visibility across the entire digital marketing ecosystem.

Measuring the success of search and social campaigns — and digital marketing as a whole — relies on metrics. Without a marketing fraud strategy in place, marketers are celebrating hitting a certain number of likes, followers or conversions, for example, but they can't be certain they're getting a true picture of success from those numbers or that ad spend.

In the case of walled gardens, advertisers believe that since they are either buying on CPA or optimizing on CPA they are protected from buying unproductive bot traffic. What really happens is the cost of bot traffic gets built into their effective CPA and creates cost inflation. Optimization algorithms gradually shift to more productive traffic but this is a slow process as it takes a while for conversion data to build up.

Marketing fraud impacts social and search metrics

Social media in particular can be a target for fake followers and fraud in its mass market nature. For example, a brand promoting a customer survey with an incentive attached is at risk, as bot operations can easily pick up on these promotions. In addition, there are companies that specialize in building audiences for social and lead generation that use suspect methods.

Larry Kotch, co-founder and marketing strategist of digital marketing agency The Brains, is creating a series of YouTube videos exposing some of these practices. He says: "There are a lot of software [companies] who say they can grow your YouTube channel or get you a million subscribers in a week, and use fake profiles to subscribe to you. The whole thing is just built on vanity metrics that don't help you in any way, shape or form."

The controversy that hit influencer marketing regarding the influx of fake followers is a recent example of marketers waking up to wasted spend. How influential is a YouTube star if 75 percent of their followers are bots? It's a similar story with ad fraud: is a campaign successful if 50 percent of the clicks measured turn out to be bots?

> **When the numbers look good, no one is questioning them — and marketing fraud makes the numbers look good.**
>
> — **Angus McLean, director, global marketing and media consultancy Ebiquity**

Driving for scale is at the root of advertisers' vulnerability

Angus McLean, at Ebiquity, says: "Advertisers are stuck in a vicious circle, pushed by the need to show results and accountability for their digital spend. [It] forces them to invest in channels that seem to drive results."

The industry wants scale at low costs, and that can open the system up to fraud. "There is a need to clear up the ecosystem, but all players are interested in maintaining the status quo and increasing the share of digital spends," says McLean. He says publishers have been forced into questionable tactics, such as buying traffic – bot or very low quality – and partnering with clickbait content companies that feed the fraud ecosystem purely to generate enough cheap impressions to feed the exchanges.

"Their business model of selling direct to advertisers for a premium can no longer compete with the likes of Google and Facebook, and the agency trading desks push cheap programmatic media that is unaccountable." add McLean. However, he adds: "Progressive advertisers are taking a step back and questioning the true value of this low cost media and realising they aren't the ones being made rich by it."

Marketing effectiveness lies in reaching humans

Marketers work extremely hard to ensure return on marketing investment and to make certain every dollar works its hardest to drive optimal business results. Awareness of marketing fraud — and the power to stop it — gives marketers a competitive advantage; it ensures hard work and hard earned budgets are not wasted on bots.

Pursuing and eliminating marketing fraud is also about developing new and wider understandings of the whole digital marketing picture — that's a collateral outcome, but important nonetheless.

As Brill, at Birmingham City University, says: "You have to take a holistic view of the whole thing. There has to be some reference to the data piece, and the ad piece and so on, because they're all linked together."

Addressing marketing fraud — in the same way the industry is actively tackling ad fraud — gives marketers the ability to optimize conversions, improve data hygiene, reduce costs and drive real human engagement. Marketing fraud is preventing true marketing effectiveness, and the remedy for digital marketers is to keep it human.

About HUMAN Marketing Integrity

Identify sophisticated bot traffic by measuring level and sources of bot activity to identify problematic lead-generation partners and initiatives. Prevent fraudulent leads by spotting fake information and match with CRM data to block fake contacts from entering sales and marketing systems. Optimize conversions by increasing conversion rates by maximizing engagement with humans, not bots. Cut costs by eliminating wasted retargeting and sales activity on bot traffic. Protect your reputation by avoiding potential regulatory penalties by preventing fake contacts from entering your automated marketing system. Maintain accurate reporting by scrubbing skewed data from your attribution reports to truly know which campaigns and partners are successful.

To learn more, visit:
https://www.humansecurity.com/products/marketing-integrity