2017 Sophisticated Invalid Traffic Assessment: The State of Ad Fraud in the Belgian Market
Thanks for reading this, fellow human. We put a lot of work into this research, and we have a big agenda: we want to make ad fraud unprofitable.

To do that, we need you to read this paper and follow the action steps. And we need to reach a really big audience.

The research was satisfying by itself, sure. But we don’t just want to know what we know. We want action. We want to improve the world by making ad fraud unprofitable. And we want your help. Your help will make advertising more effective for advertisers and more fair for great content creators. And it will take a big bite out of the profits of cybercriminal botnets, which will be good for everyone. That takes action, not just knowledge. So... we need to reach that big audience.

We will all be looking at our analytics dashboards to see how many pageviews this paper is getting. Every day. I will be asking how this paper is trending. No matter how wide it goes, I will be asking what else we can do to get more hits.

Like us, everyone with something to promote wants more pageviews, more visitors, more reach. And that’s why bot fraud exists.

The fundamental problem is this: if you want more visitors to a website, you can just buy them. Everywhere that publishers pay for visitors, we find fake visitors. Those fake visits come from bots, and they can be made to look very convincing. Bot traffic is great for pageviews, for clickthroughs, for view rates, and for filling any kind of demographic, geographic, or interest target, no matter how unlikely. But bot traffic is not great for real world action.

But bots don’t show up in big numbers unless they’re paid for. Our research here casts this into stark relief. The Belgian market is substantially cleaner than the global average because the practice of buying visitors – traffic sourcing – is far less common among Belgian publishers.

Eliminating bots entirely from the Belgian media landscape can happen much faster here than any other market we have ever studied. This is an exciting opportunity. Thank you for your attention. And your actions to take this achievement the rest of the way!

Michael Tiffany
CEO/Co-Founder
In 2014, White Ops worked with the U.S. Association of National Advertisers (ANA) to conduct the first-ever, large-scale survey of fraud in online advertising. Together, we found that criminal operators had infiltrated the U.S. advertising ecosystem to redirect large amounts of advertisers’ budget and traffic to bots. At the time, we discovered that about 6 percent of the average participant’s overall web traffic came from users who were not human.

Further, specific categories of advertising encountered even higher fraud rates - 23 percent of video advertising, 19 percent of retargeted advertising and 17 percent of programmatic advertising came from bots. Overall, the prevalence of invalid traffic was unlike anything we had ever seen before.

Since our report in 2014, White Ops has continued to monitor, educate, and fight against this growing threat. While the U.S. market is currently a high focus for fraudsters, we wanted to examine whether this breakdown was also evident in other global markets. This latest study, in 2017, is a collaboration between Accenture, a leading global professional services company, the Unie van Belgische Adverteerders (UBA) and White Ops to evaluate the level of fraud currently encountered by UBA members in the Belgian market. Using White Ops technology, the study evaluates the level of advertising fraud facing Belgian companies, based on 248 million advertising impressions from UBA members between January and February 2017.

Over the course of our study, UBA advertisers encountered very little fraud in most cases — yet elevated fraud rates came from certain publishers, traffic from specific countries and traffic from individual domains.
Top 5 Findings

1. The overall fraud encountered by UBA members is low.

2. Ad impressions served outside of the E.U. result in higher fraud rates.

3. Smaller campaigns encounter a greater range of fraud.

4. A single publisher sourced significant fraud.

5. One participant had significantly higher levels of SIVT than the others.

Smaller campaigns encounter a greater range of fraud.
Across the entire study, SIVT accounted for only 2 percent of all non-mobile advertising activity measured, and the average advertiser saw just 1.9 percent of their ad impressions come from fraud.

This finding indicates that Belgian advertisers encounter little fraud compared to other markets, such as the U.S., where fraud levels ranged from 3 to 37 percent, according to prior research by White Ops.
UBA Study Top-Line Results

![Bar chart showing UBA Study Top-Line Results]

- Impressions (Millions)
- SIVT %

The chart displays the impressions (in millions) and SIVT % for different participants.
Approximately 21 percent of impressions coming from U.S. domains — nearly 180,000 total impressions — appear to be fraudulent invalid traffic from non-human sources. Additionally, Russian sources generated 26 percent SIVT, though it represented a smaller sample size of about 15,000 total impressions.

When an advertisement is placed online, the audience for that ad can come from anywhere in the world. However, not all traffic is created equal.

White Ops analyzed the fraud rates of UBA advertisers for traffic originating from other countries. We found that when sources from Europe send traffic to Belgian advertisers, fraud appears to be moderately higher, on average.

However, fraudulent traffic from the United States and Russia is significantly higher than European nations.
Fraud Rates for Traffic Originating Outside of Belgium

- Belgium's 4.4 million SIVT impressions extend past top of chart

- Belgium: 26.2% SIVT
- United States: 2.0% SIVT

Legend:
- Orange bars: SIVT Impressions
- Black dots: SIVT %
This study found that larger campaigns tended to have less overall fraud. Due to greater variability, many smaller campaigns had higher fraud rates, topping 10 percent.

Advertisers tend to categorize purchases with a specific goal into a single campaign. As such, campaigns tend to be the basic unit of measurement to determine whether an advertiser’s policy and technology is able to discern fraudulent traffic.

One possible reason for higher levels of fraud in smaller campaigns is that many marketers are targeting niche audiences, which makes them more susceptible to shortfalls in human audiences. By targeting a small group of users, the probability of reaching real humans in that subset is low – meaning you’re likely
Smaller campaigns tend to have higher fraud rates. As such, this makes niche audiences a lucrative target for bot operators. Conversely, larger campaigns distribute their advertising dollars over a wider variety of publishers, which offsets the impact of those with large fraud rates.
When analyzing this data, we found three specific sites that were responsible for generating high rates of SIVT. Advertisements hosted on those sites saw 45 percent, 43 percent and 46 percent SIVT during the study period. All three sites belonged to the same publisher and created significant losses for advertisers.

The advertiser encountering the greatest level of fraud in the study — nearly 9 percent — received traffic from two of the publisher’s three sites. While the advertiser had a small sample size of less than 10 million impressions during the study period, such a high fraud rate could cost this advertiser significantly, and could continue to do so in future campaigns.

The data underscores the influence publishers have on the level of invalid traffic. Therefore, pushing publishers to focus on eliminating fraud could make a large difference in overall fraud rate. Publishers with high SIVT should be avoided until they can better mitigate the problem of sophisticated invalid traffic.
Fraud by Publisher

![Graph showing impressions and SIVT % for publishers.](image)

- Impressions (millions)
- Publisher

Key:
- Orange bars: Impressions
- Grey dots: SIVT %

44.4%
Our data concluded that several providers’ domains had much higher sophisticated bot traffic than the norm.

Two sites accounted for a total of 1.1 million impressions and allowed about 36 percent SIVT each to UBA participants’ display ads. Another campaign from a single publisher consisted of 180,000 impressions and resulted in 79 percent non-human traffic. Finally, a fourth site allowed over 600,000 impressions, and garnered 19 percent invalid traffic being charged to advertisers.

While most SIVT in the Belgian market came from small fraud rates within very large-volume providers, we discovered that a significant amount of this type of fraud actually came from four smaller providers with a high rate of SIVT.
Fraud Rate for Domains

![Graph showing the fraud rate for domains in Belgium, with bars representing impressions and a line indicating SIVT% with a peak at 78.9%.]
Additional Insights
Programmatic and Direct Advertising Encounter Average Fraud

More than 90 percent of desktop-focused advertising came from programmatic and direct campaigns, and the fraud associated with those buy types matched the average study SIVT seen by participants.
Viewability: Not all bots are created equal.

While viewability of human verified impressions were clustered within expected norms, invalid traffic viewability was much more inconsistent. This uneven distribution differs from other markets, such as the U.S., where botnet operators have developed more sophisticated methods to purposely spoof viewability measurement with the goal of appearing more human.

Reasons for this type of effort to fake viewability measurements could be that the Belgian market isn’t yet seen as a valuable entry point for more dangerous botnets, or that the detection measures employed are not challenging enough for fraudsters to manipulate for their personal gain.
Viewable Rate by Campaign and Impression Type
Display advertisements that came from desktop systems had a fraud rate of 1.6 percent, which is lower than the average SIVT rate in the study (2 percent). Advertising traffic that did not have a discernible device type, however, had a higher fraud rate of 3.1 percent. Further, impressions intended for desktop, but were actually served on mobile, had an even higher fraud rate of 6.5 percent.

Additionally, the research showed that 98 percent of traffic, and most of the fraud found in UBA campaigns, was directed at desktop display ads. This is consistent with data from surveyed companies, indicating that advertisers commit more than half of their budget to desktop display and video advertising, and much less to mobile advertising. As mobile is a growing area of investment for all advertisers, it deserves additional monitoring.
Fraud by Device Identifier

- Desktop: 150 (Impressions, SIVT %)
- Unclassified: 50 (Impressions, SIVT %)
- Mobile: 10 (Impressions, SIVT %)
Conclusion
Where Do We Go from Here?

It is encouraging that the Belgian market has low overall fraud, and it’s something White Ops would like to see in other global markets, as well. However, we must not take this lull in criminal activity for granted, as it does not protect advertisers from future incidents.

It’s important to note that about 90 percent of the impressions in this study came from programmatic and direct display advertising. For comparison, U.S. advertisers have shown to focus 68 percent of their advertising volume on those two types of ad buying – opting to also include video display advertising into their promotional mix (seen from past research).

This underscores the pervasiveness of bot fraud in video advertising. Since traffic sourcing is so low among the participants, and video display advertising was not a primary focus, the overall fraud encountered by UBA members is very low. In the U.S. market, video advertising is extremely lucrative, making it a bigger target for fraudsters.

UBA advertisers saw the greatest fraud in the lower-volume buy types. Also, note that advertisers who do not monitor or tag their traffic — those whose buy types could not be discerned — are subject to higher rates of fraud.
Key Takeaways

- UBA advertisers saw less fraud with programmatic and direct display ads, a contrast to U.S. advertisers
- Smaller ad campaigns tended to have higher fraud
- One advertiser encountered a much higher degree of fraud (three times the next highest level)
- Several campaigns had significant levels of fraud
- Certain publishers and sites had much higher levels of fraud, nearly 80 percent in one case
- As video investment grows in this market, it represents another area to monitor, as it has driven higher fraud in other markets
Learning from History

Advertisers should remember that fraud does not just happen without prompting — it occurs when criminal operators see untapped demand that they can fill with fraudulent advertising. In White Ops’ experience, the top cause of fraud is traffic sourcing, which is not currently evident in the Belgian market, based on evidence we uncovered.

We’ve seen this play out on a global scale in advertising markets like the United States and Russia. With the ever-growing demand for more traffic, along with high mobile and video consumption, incentive is high for publishers to source content and traffic however they can. There is a lucrative market in mobile and video ads, and, thus, a low-risk high-reward opportunity for bot operators. That’s how we end up with massive botnets like Methbot. As traffic sourcing inevitably grows in the Belgian market as well, and mobile and video content become more ubiquitous, advertisers should expect their fraud rates to grow as well.
An Opportunity for Change

Traffic sourcing is far less pervasive here, than in the U.S. So, while this represents a significant untapped market for fraudsters, it’s also an opportunity for publishers and policy-makers to adopt new security measures and software platforms to help minimize the impact of frauds in the future.

When publishers start sourcing traffic, it creates a slippery slope and opens the door to some of the world’s most elite cybercriminals. But, if we can prevent that process before it begins, and arm buyers with enough technology to identify where a publisher is buying traffic, we can address the issue at the media planning stage to maximize leverage against these cybercriminals.

It’s infinitely easier to stomp out fraud entirely if we can detect it early and take steps to combat it proactively, rather than remaining complacent and reflexively reacting once it’s already taken hold in the market.
Appendix
Traffic Sourcing Impact on the Digital Advertising Supply Chain

What is Traffic Sourcing?

A common tactic used by digital publishers to increase impressions delivered or engagement to web pages. Traffic sourcing is the practice of buying "visitors" from specialized brokers. These brokers sell site visits for fractions of a cent as high engaged, targeted and qualified human audiences. Unfortunately, most, if not all, of this traffic is bot driven. Once in the digital supply chain, it negatively impacts all stakeholders.

Each fraudulent incident occurs in a matter of milliseconds and is most often undetected by the marketplace. Botnet operators automate this process to repeat at scale millions of times per day resulting in extensive reach of fraud.
### SOURCES OF BOTS
- Bot Script
- Botnet running off of malware infected devices, largely residential computers

### PHANTOM LAYER
- Phantom Websites
- Anonymizing network or proxy

### SUPPLIER
- Seller of Traffic
- Provides what the broker requests, often clicks

### BROKER
- Broker of Traffic
- Service-oriented media companies that do campaign management and audience extension

### PUBLISHER
- Buyer and Reseller of Traffic and clicks
- Both premium and longtail sites and networks
- Measured impressions

### ADVERTISER OR AGENCY
- Buyer of Media Placements

---

#### Phantom Layer Traffic Mixes with Legitimate Traffic

- Large PPC Network
- Impression Handlers (platforms and exchanges)
- Anonymizing Search Engine Traffic
- Audience Extension or Other Supplier Network

---

Network and Exchanges
- Networks
- Exchanges
- Secondary Phantom Site

Publisher
- Publisher
AD
AD
AD
Methodology

The study collected data from UBA member advertisements using White Ops technology from 15 January 2017 to 15 February 2017, for a total of more than 248 million impressions.

Because mobile advertising uses different frameworks and platforms for monetizing traffic, White Ops excludes ad traffic originating on mobile devices in its studies. Overall, mobile accounted for about one third of the impressions seen by all UBA participants.

White Ops limited analysis to those campaigns with more than 10,000 impressions. One campaign of 680 impressions had a 100 percent fraud rate, but was not included in our final analysis. Because the UBA data set had very little video traffic, video buys were excluded from the analysis as well.
Demographics

The surveys conducted by White Ops and Accenture of UBA participants found that advertisers rated advertising fraud an important problem to solve, giving it an average rating of 4.3 on a scale of 5, with 5 being the most important. However, the companies lacked confidence in their anti-fraud solutions, rating the technology only a 2.2 on the same scale.

On average, companies use two-to-three different viewability and fraud-detection solutions, with the average company (median) using two solutions. Most advertisers access their viewability reports at least every month. On the other hand, most advertisers do not access their fraud reports at all, instead leaving that measurement to their agencies. Every company used DoubleClick for either brand safety or viewability.

Nearly all advertisers who participated in the study targeted every age group as well as the high-income demographic. More than 44 percent of advertisers also targeted small business, but no advertisers specifically targeted minorities. The top three considerations in media buys were brand safety, the ability to track sales both online and offline and viewability measurements, according to survey responses.
Impressions/Fraud for Study Period

![Graph showing Impressions and SIVT % over weeks from Jan 10 2017 to Feb 14 2017](image-url)
Glossary

**Gross Impression**: Sum of Decisions and Incomplete Loads.

**Decision**: Deterministic identification of a particular impression, page view, or other type of online event as invalid traffic (IVT) or human.

**General Invalid Traffic (GIVT)**: Routine known non-human or fraudulent sources through industry lists such as the IAB Bots & Spiders list, as well as parameter-based techniques.

**Sophisticated Invalid Traffic (SIVT)**: Impressions identified by browser, app or session behavior and other attributes that are inconsistent with a valid human behavior.

**Sourced Traffic**: Any method by which digital media sellers acquire visitors through third parties. With sourced traffic, a publisher pays a third-party vendor to send users to its site by advertising on other publishers’ sites.

**SIVT %**: Percentage of decisions determined to be Sophisticated IVT (Sophisticated IVT / Decisions)

**Domain**: A unique name that identifies and can be used to access an internet resource such as a website.

**Publisher**: The operator of a website or network of websites, and the producer or curator of content for those sites. A seller of online advertising space and impressions, and often a buyer of third-party traffic.

**Site or Website**: A set of related web pages, often served from a single domain.
ABOUT UBA

UBA is the Belgian organisation made by brands, made for brands. Today, the UBA member community consists of 300 companies who account for the majority of national media investments. As a result, UBA is a unique platform enabling its members to protect the interests of brands and engage in the exchange of knowledge. Through its extensive range of activities and services, UBA stimulates a creative, innovative and transparent communication ecosystem enabling strong and sustainable brands.

In the development of its activities and services, UBA consistently implements four strategic principles: inspire, impact, enable and connect. These principles guarantee a relevant service that makes brand builders stronger.

ABOUT ACCENTURE INTERACTIVE

Accenture Interactive is part of Accenture, a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Accenture Interactive helps the world’s leading brands transform their customer experiences across the entire customer journey. Through our connected offerings in design, marketing, content and commerce, we create new ways to win in today’s experience-led economy. Accenture Interactive was ranked the world’s largest and fastest-growing digital agency in the latest Ad Age Agency Report. To learn more follow us @accenturesocial and visit www.accentureinteractive.com.
ABOUT WHITE OPS

White Ops is the global leader in human verification and data integrity. In 2016, White Ops was the first company to receive MRC accreditation for Invalid traffic detection paving the way for the industry and offering a full suite solution that includes viewability, brand safety, fraud detection, and pre-bid verification. Working with some of the best hackers and ad tech specialists in the world, we’re able to think outside the box and create the best solutions for our clients.

New York | Victoria | San Francisco
Atlanta | Los Angeles | Chicago

www.whiteops.com
info@whiteops.com