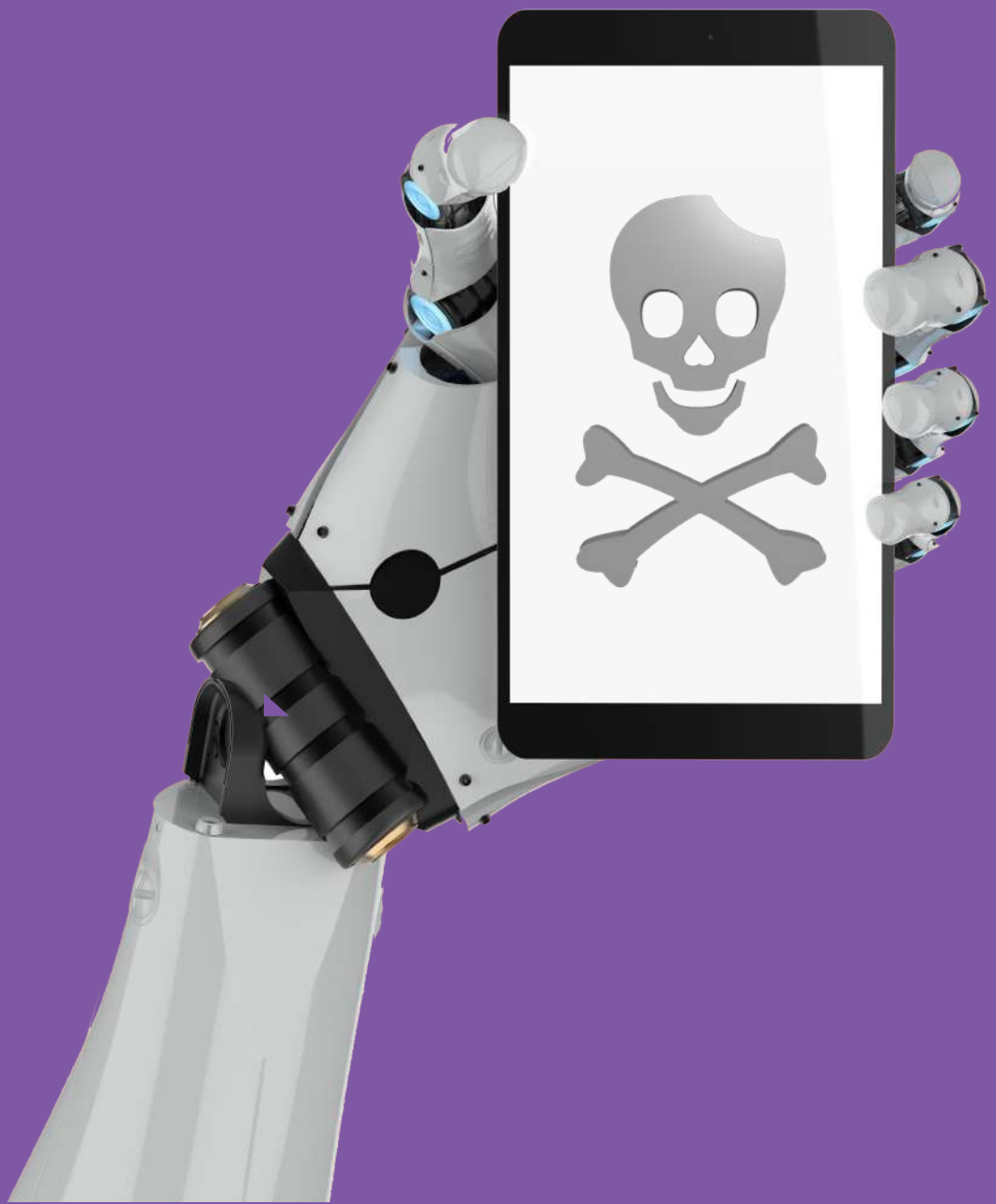
WUNDERWORX
AD BUYING MADE SIMPLE

PRESENTS: MARKETING MATTERS, VOLUME I

THE TRUE COSTS OF ONLINE AD FRAUD

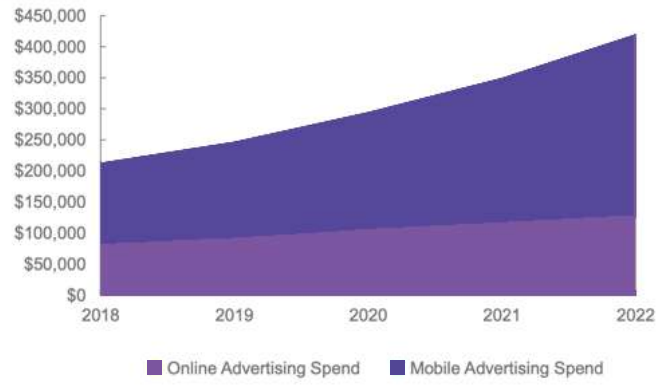
SECOND EDITION



INTRODUCTION

For those of you who have been keeping up with online advertising, chances are you aware of the reported costs associated with **online ad fraud**. This fraud takes on many forms such as wasted media ad dollars, falsely reported app installs and bot-driven clicks by non-human users. Individually, the cost is minuscule, but collectively, it is significant. While the costs may be difficult to quantify, Juniper Research predicts that by 2022, the loss to mobile advertising fraud is forecasted to reach **$87 billion** globally.[1]

Global Online & Mobile Advertising Spend (US$m)



Source: Juniper Research

To make digital advertising campaigns successful, marketers need to ensure their ad spend is being used to reach real people. The most common form of ad fraud is bots or domain spoofing. According to IAS Insider, marketers should be vigilant ahead of the Christmas holiday shopping season. Additionally they warned that brands should be aware of the risk accompanying video ads.[2]

Ad fraud is complex. As the advertising industry develops new technology to detect suspicious activity, fraudsters continue to stay one step ahead. So it's no surprise advertisers, agencies, and tech partners, frustrated by the difficulty of fraud identification, are increasingly inclined towards knee-jerk blocking. According to IAS Insider, **knowledge is the best defense**.[3] SDK Spoofing and Install App Farms will continue to be a major concern for mobile app advertisers. This issues expected to increase, with **1 in 10 app installs** expected to be fraudulent by 2022.[4]

Within the broad scope of online criminal activity, online ad fraud has incredibly high payout and remains very difficult to penalize by law—only complicated by most ad fraud is committed in countries with infective law enforcement. The bottom line is that your ads and your app installs should be seen and downloaded by real people—not bots. As creative as marketers can be in extending your brand message, ideating advertising campaigns, building highly targeted audiences, so can fraudsters in their schemes to defraud brands. Learn how **WUNDERWORX** can help prevent ad fraud and **eliminate wasted ad dollars**.

Steve Nolan
CEO & Founder, **WUNDERWORX**, Inc.

"The level of criminal, non-human traffic literally robbing marketers' brand-building investments is a travesty."

- **BOB LIODICE**, President & CEO Association of National Advisors

DIGITAL ADVERTISING HAS BALLOONED INTO A $100 BILLION INDUSTRY WITH MANY MOVING PARTS CONTRIBUTING TO IMPRESSIVELY HIGH GROWTH. HERE'S HOW IT HAPPENED:

It's no surprise that in such a fast-growing industry, fraud would be such a systemic problem. Online targeting **click farms**, **clickbots** and **viewbots** come in many shapes and sizes. Studies have found that as much as **1/3 of all internet web traffic** is generated by bots making phony impressions and fraudulent clicks, which costs companies billions in ad spends.[2] But how many of those clicks, views, and streaming videos are generated by actual people exploring to make a purchase, and how many are fake click-bots costing companies billions in fraudulent ad spend every year?

A recent study by Juniper Research, by 2022, the total loss to mobile advertising fraud is forecasted to reach **US $87 billion**, rising from **US $34 billion** in 2018.[8] Display media with $10 cost per thousand impressions (CPM) had **39% more** bots than media with lower ad prices. The upper end of video, where CPMs are generally higher, had **173% more bots** than lower-CPM video media. Programmatic ad buying saw eve saw even more bots.[9]

- US digital ad sales are expected to grow by **15%+** this year to pass the **$100 billion** milestone (**52%** of total ad sales).[6]
- Mobile ad spending represented **57%** share of the total digital advertising in 2017.[7]
- In 2017 digital advertisers lost **$39 million** per day to fraudulent activities, as these undergo continuous innovation to avoid detection.[4]
- Digital video increased **33%** in 2017 to a record **$11.9 billion**. On mobile devices, video revenue surged by **54%** to **$6.2 billion**, representing the first time that mobile video revenue surpassed desktop video.[7]
- Social Media advertising brought in **$22.2 billion** last year, growing by **36%** from **$16.3 billion** in 2016.[7]
- Search revenue rose **18%** to **$40.6 billion** in 2017.[7]
- Banner advertising rose **23%** to **$27.5 billion**, **67%** of which came from mobile.[7]
- According to the Word Federation of Advertisers (WFA), it is estimated that by 2025, over **$50 billion** will be wasted annually on ad fraud.[5]

HOW MUCH ARE BOTS COSTING

The fraud ad bot network is estimated to cost advertisers over **$6 million a month** and is growing at alarming rates, **78% of marketers**, whose losses amount to billions in digital ad fraud, cite click fraud and bot traffic as their top concerns. According to the World Federation of Advertisers estimates, if digital ad fraud is not effectively addresses, the potential yearly lost revenue could reach **$50 billion** in the next 10 years.

CLICK FRAUD STATISTICS

- **1 in 5** ad-serving websites are visited exclusively by fraud bots.[10]
- **20%** of pay-per-clicks are fraudulent.[11]
- Nearly 20% of total digital ad spend gets wasted each year.[12]
- **$1 in $3** spent on digital ads are fraudulent, accounting for **$6.5 billion** in ad fraud in 2017.[13]
- **50% of online ads** are never seen by human eyes.[15]
- Only **43%** of the industry say they understand how fraud is detected.[16]

WHY SHOULD YOUR CARE?

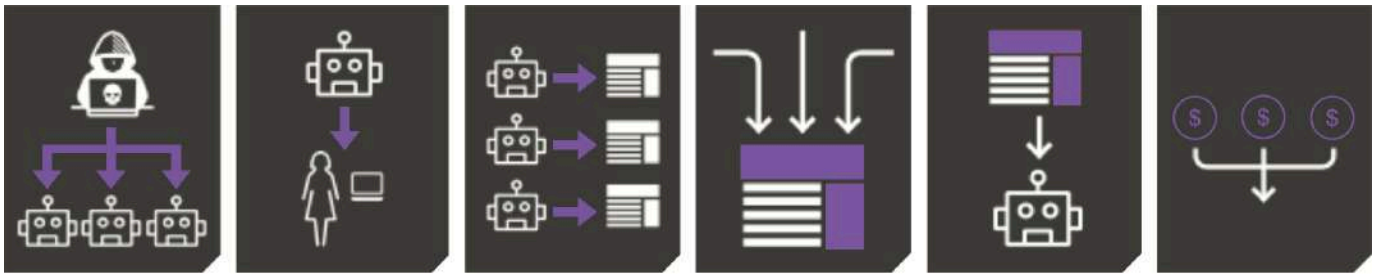
Considering the problem's severity, it's hard to believe that currently, these bots are entirely legal. That in itself is among the biggest reasons the fraud is so rampant. Unlike credit card fraud, nobody is going to jail for ad fraud, and it is extremely lucrative.[17]

It is big business. The click fraud operation Methbot is based in Russia and operates out of data centers in the United States and the Netherlands, this notorious "bot farm" generates **$3 to $5 million** in fraudulent revenue per day by targeting the premium video advertising ecosystem.[18] But it's not alone. Click Monkeys, working out of Ukraine, has a giant tanker click farm stationed in international waters off the coast of San Francisco and is not subject to any U.S. laws.

"I'M REALLY NOT WORRIED ABOUT WHETHER ADVERTISING WILL BE ABLE TO FIND ITS WAY THROUGH DIGITAL CHANNELS. I AM CONCERNED—VERY CONCERNED—VERY, VERY CONCERNED—THAT COSTS OF ADS WILL GO UP AND UP AND UP FROM THIS UNETHICAL OBSTRUCTION."

- RANDALL ROTENBERG, CEO Interactive Advertising Bureau (IAB)

HOW DOES FRAUDULENT TRAFFIC OCCUR?



Hackers use code to create bots that are able to take orders from botnet center

Users unknowingly download and install bot engines on their computers.

Bots are instructed to visit premium sites, picking up desirable cookies, and then visit fraudulent sites.

Highly trafficked fraudulent sites use exchanges and networks to attract advertisers.

Ads are continuously served to bots.

Botnet operator gets paid.

BUYER BEWARE

According to a study by eZanga, **37% marketers** have absolutely no idea where ad fraud originated.[19] For example, the U.S. State Department spent **$630,000** on Facebook to acquire **2 million followers**, but then later learned that their engagement was only a **2%**, they realized their spend had only gotten then fake followers.[20]

AD FRAUD COMES IN MANY SHAPES AND SIZES, WITH MANY GUISES. LISTED BELOW ARE MANY OF THE MORE POPULAR FORMS:

- **AD INJECTION** involved inserting ads into an app, webpage, or other form of media without the consent of the publisher or operator. The ad can be visible or hidden.[21]
- **AD STACKING** is a fraud where multiple ads are stacked on top of one another in a single ad placement. While only the top ad is visible, if a user clicks on it, one is registered for all ads in the stack.
- **CLICKBOTS** are a type of Malware. Once installed on a device, it will automatically browse the web and click on pay-per-click ads.
- **CLICK FARMS** are usually located developing countries with very low wage rates. Workers are paid to manually click on ads, earning about **$300 to $400** a year.
- **COOKIE STUFFING** can happen in different ways. One method is to place multiple cookies on a user or bot so that they get targeted at a higher cost per thousand.
- **PIXEL STUFFING** occurs when serving one or more ads in a single 1x1 pixel frame, so that they ads are invisible to the naked eye.

- **LOCATION FRAUD** is when an advertiser pays for inventory to be served in a particular country or region, but the traffic is actually served elsewhere.
- **MOBILE SIMULATORS** are a sophisticated form of fraud that are designed to mimic smartphone activity and are used to create phony traffic on in-app mobile ads.
- **RETARGETING FRAUD** imitates human users by falsely appearing to have an interest in a specific brand for targeting
- **MALWARE** is malicious software that runs silently on infected computers that click ads on websites. According to Threat Report, *"Part of the exponential growth of malware, and the bulk of the attacks on various industries, can be attributed to the continued rise in polymorphic and single-use malware."* Single use, targeted malware let cybercriminals attack with greater precision and to remain hidden.
- **DOMAIN SPOOFING** is commonly used to mask unsafe sites. Fraudsters can spoof the domains of sites like video piracy sites in order to conceal their real identity and monetize the traffic.

HOW TO REDUCE YOUR RISK OF AD FRAUD

Preventing click fraud is not as difficult as it seems. The sooner you are aware of the problem, the sooner you can find the problem and reduce or eliminate further damage. Today, there's malware designed to generate it and brokers who sell it. Some companies pay for it intentionally, some accidentally, and some prefer to just not ask where their traffic comes from. It has given rise to an industry of countermeasures, which inspire counter-countermeasures.[22] Be on the lookout for sudden spikes in traffic—especially during certain times of the day—that establish a pattern, could be a red flag.

At **WUNDERWORX**, we believe one effective way to reduce wasteful spending on fraudulent ads is to design mobile ad campaigns that use intent-based targeting. Mobile intent-based targeting yields a **20% higher ad recall lift** and **50% higher brand awareness lift**, relative to campaigns that purely target by demographics. When buying ad inventory, we use a combination of Google's intent and interest data combined with our hyper-focused geo-spatial capabilities. This allows us to better determine **geo-intent** by factoring in **geo-location patterns** to find audiences that are of the right mindset and profile for your brand.

INTERESTED IN LEARNING MORE?

WUNDERWORX is helping agencies and small businesses take control through our self-serve ad buying platform. **WUNDERWORX** provides the power of real-time programmatic advertising campaigns across all devices and media, leveraging sophisticated **geo-spatial audience building** technology from our **easy-to-use dashboard**. Give us a call and let us demonstrate how **programmatic**, **paid search** and **SEO** can help you grow your business.

THE TRUE COSTS OF ONLINE AD FRAUD

BY: **STEVE NOLAN**, CEO & CO-FOUNDER
Contact Us: Hello@Wunderworx.io
wwww.wunderworx.io
888.470.7870

SOURCES:

1. **Source:** https://insider.integralads.com/uk/our-latest-uk-media-quality-findings-for-h1-2019/
2. **Source:** Vraanica, Suzanne, March 23, 2014, The Wall Street Journal: https://www.wsj.com/articles/the-secret-about-online- ad-traffic-one-third-is-bogus-1395684863
3. **Source:** https://insider.integralads.com/uk/how-to-tell-the-difference-between-friend-and-fraud/
4. **Source:** Juniper Research, Addressing Ad Fraud Through Multipoint Analysis & Machine Learning
5. **Source:** Ad Fraud Essentials, IAS Integral Ad Science
6. **Source:** Bertwitz, Scott & Letang Vincent, June 18, 2018: https:// magnaglobal.com/video-global-ad-forecast- june-2018/
7. **Source:** IAB Internet Advertising Report: https://www.iab. com/ news/digital-ad-spend-reaches-all-time-high-88-billion- 2017-mobile-upswing-unabated-accounting-57-revenue/
8. **Source:** https://www.juniperresearch.com/press/press-releases/ advertising-fraud-losses-to-reach-42-bn-2019
9. **Source:** Slefo, George, January 19, 2016, Ad Age, http:// adage.com/article/digital/ana-report-7-2-billion-lost-ad-fraud-2015/302201/
10. **Source:** Brandom, Russell, May 24th, 2017, The Verge: https:// w w w . t h e v e r g e . c o m / 2 0 1 7/ 5 / 2 4 / 1 5 6 8 1 0 8 0 / a d - f r a u d - w e b s i t e s - traffic-bots-white-ops-report
11. **Source:** http://blog.pixalate.com/desktop-ad-click-fraud- rising-stats-data-2017
12. **Source:** Handley, Lucy, March 15, 2017, https://www.cnbc. com/ 2017/03/15/businesses-could-lose-164-billion-to-online- advert-fraud-in-2017.html
13. **Source:** Ad Age, January 08, 2018: http://adage.com/article/ news/ 2018-predictions/311833/
14. **Source:** Marinch, Terenty, https://blog.adbeat.com/display- ads/
15. **Source:** Schuman, Loni, June 2018, https://www.clickcease. com/ blog/click-fraud-statistics/
16. **Source:** Ad Fraud, A Short Guide, Integral Ad Science, http:// integralads.com/uk/wp-content/uploads/sites/5/2017/01/ IAS_Ad-Fraud-101-Guide_UK.pdf
17. **Source:** Napier, Bill: January 16, 2018, https://www. themarketingscope.com/buyer-beware-digital-ad-fraud-is-everywhere/
18. **Source:** https://www.whiteops.com/methbot
19. **Source:** http://blog.ezanga.com/blog/an-ezanga-survey-finds-37-of-marketers-are-unsure-about-where-ad-fraud-originates
20. **Source:** https://www.washingtonpost.com/news/federal-eye/ wp/ 2013/07/03/ig-report-state-department-spent-630000- to-increase-facebook-likes/?noredirect=on&utm_term=. a021cd809f3d
21. **Source:** IAS Team, April 25th, IAS Insider, https://insider. integralads.com/ad-fraud-glossary/
22. **Source:** Bradley, Tony, May 4, 2018, Forbes, https://www. forbes.com/sites/tonybradley/2018/05/04/new-threat-report-highlights-concerning-malware-trends/#380c09422957