THE $180 BILLION HEIST THAT HAPPENS EVERY YEAR, IN BROAD DAYLIGHT

Hello to all my new readers –

The headline for this "explainer" is deliberately provocative. Because the subject matter is *so* super-nerdy that most people glaze over after a few minutes.

Which is how the Bad Guys win.

EXECUTIVE SUMMARY OF THE PROBLEM:

1. The global internet advertising market is between $640 - $720 billion/year. Projected to reach 1.165 TRILLION by 2030. Source: https://www.grandviewresearch.com/industry-analysis/digital-advertising-market-report

2. Lowest-end estimate is that at least 20% of the clicks on those ads are fraud (this study is from AdWeek, a mag whose audience is ad agencies, and thus, perhaps not wanting to admit how bad the problem is) https://www.adweek.com/programmatic/why-ad-fraud-rates-havent-budged-in-15-years/

3. A more balanced report cites 36% of ad traffic as "IVT" (InValid Traffic, aka bots) https://gitnux.org/ad-fraud-statistics/ (Video ad traffic fraud rate is cited as 50%!!! Which is utter madness, and the ENTIRE U.S. video ad industry is in the process of shifting their spend from broadcast 30-second spots, to ads on streaming platforms. Lured by the promise that these ads are "trackable." Spoiler: it's 90% fraud right now.)

4. Anura cites 40-50% as the stat for ad fraud, with the losses to hit $200 BILLION by 2028 https://www.anura.io/ad-fraud-ultimate-guide/ad-fraud-statistics

5. Ad Agencies are NOT interested in blowing the whistle and derailing the gravy train, and actively discourage their employees from revealing too much: https://cubera.co/the-rise-of-transparent-advertising-why-its-non-negotiable-in-2025/

6. The publishers had NOT updated their agreements with digital ad platfoirms since 2001: https://www.billhartzer.com/advertising/after-24-years-iab-wipes-the-slate-clean-on-digital-ad-agreements/

7. Some big social media platforms are starting to feel the heat – SnapChat is trying to verify that the (claimed) 469 million users are actually human beings, and that the ads are not just crammed down below the screen where no humans can see them: https://www.billhartzer.com/advertising/ias-snap-advertisers-proof/

WORK THE NUMBERS:

Low-end estimate: 640BN x 20% fraud = **$120BN/yr being stolen**

High end estimate for 2030: 1.1TRN x 50% fraud = **$550BN/yr stolen**

That's a lot of money.

And it's been happening since the very beginning – see my interview with Dr. Augustine Fou: https://www.youtube.com/watch?v=pHZuFRseYsg

WAIT. HOW CAN THIS BE HAPPENING?

Dave's story: starting about 2012, I had a series of conversations with colleagues at CNN, NBC, Fox, LA Times, etc. I was just then getting into measuring website traffic using Google analytics, and I kept seeing weirdness in the traffic stats when I looked at what was happening on news sites.

Colleagues: "Oh. Yah. That's just the spikes you get when the Traffic Acquisition Manager has to make his numbers."

Dave: Wait. What? What is a Traffic Acquisition Manager?

Turns out that publishers and big website owners play a sneaky game with their advertisers. At the beginning of the month, big advertisers come to CNN/NBC/Fox/etc. and say, "We want to buy 500 million ad impressions this month. We want our logo and new product on the page every time someone comes to your site."

Cool, cool.

Flash-forward 3 weeks. There's only been 200 million impressions so far this month. Unless we get another 300 million pageviews in the next week, the publisher/TV network is gonna hafta cough up $X million in "give-backs" to the advertiser.

That ain't. Gonna. Happen.

So the publisher turns to the Traffic Acquisition Manager and says, "We need 300 million pageviews in the next week. Go get 'em."

The manager then calls on guys with Russian/Chinese/Iranian accents and a conversation ensues. Money changes hands.

Alakazam! The site gets hit with an absolute FLOOD of traffic, the pageview counter is spinning like crazy, and the website makes its quota.

Only …

That traffic? It's coming in from old Windows XP computers running a hacked version of Internet Explorer with Flash enabled. (The dirty secret of most businesses and schools in 3rd-world countries is that they run computers on hacked versions of Windows software because 1) it's cheaper and 2) **the people in charge stole the money for the legal versions of the software**).

Said computers are easily compromised by hackers and form the backbone of armies of bots.

That's the weirdness I was seeing in Google Analytics. I blinked in shock.

Dave: Um. Isn't that fraud?

Colleague: Yeah.

Dave: But … do people know about this?

Colleague: Yeah. Everybody knows because everybody does it. About 30% of all the ad clicks on the internet are total fraud. Lot of it is by foreign governments. Chinese, Russians. Hell, **this is how the North Koreans pay for their nuclear weapons program.** Meh. Whatcha gonna do? (shrug)

Dave: But … but … *(I couldn't think of anything to say at that point)*

WHAT DAVE TRIED TO DO

Running the numbers in my head, I realized that the amount of money being stolen (even in 2012) was enormous. I was teaching Digital Immersion at USC-Annenberg, and I tried to get the professors and administrators there interested in doing a research project to verify what I was being told. Journalist's motto carved into my brain: "You COULD check it out."

After all, this could just be people inflating the problem for their own personal agendas.

Nobody was interested in pursuing this. "Too technical" and "Inside baseball."

As the years passed, I got used to seeing weird traffic spikes, and read extensive comments in data/analytics forums on how to spot bots and try to filter them out.

Year after year, the bots got more sophisticated, to evade the simple gatekeeping measures that were rolled out. I learned more about how the anonymous nature of online digital advertising works, and how that has enabled Bad Guys to have a license to steal.

Once again, it's probably necessary to have a bit of a background explainer.

HOW ADVERTISING WORKED BEFORE THE INTERNET

Posit: Ford (or any other car company, really) has a new model F-150 pickup truck it wants to sell.

Ford goes to TV networks, radio stations, magazines and newspapers, and meets with the ad sales manager(s) with whom Ford has a decades-long relationship.

The two old dudes go out for a 3-martini lunch, smoke cigars, and then shake hands. Ford has just bought $50 million in ads to run over the next 3 months to alert the public that a new & improved F-150 is hitting the market.

(Aside: The Ford guy probably also gets a kickback under the table from the grateful ad sales manager, maybe a 3% slice of Ford's ad budget that he quietly splits with the TV/radio ad sales manager, but let's just avoid that rabbit hole for now.)

Ford ownership sits back and sees the ads play on TV, hears them on the radio, sees the glossy full-color pages in magazines and papers. The ads are running! How many people see them or actually pay attention rather than changing the channel/flipping the page?

We don't know. But more people show up in the Ford showrooms, so they MUST be working, right?

There's an old-time advertising saying: "I know that 50% of my ad spend is completely wasted. I just don't know which 50%."

The internet was supposed to change that.

HOW INTERNET ADVERTISING WORKS TODAY

Posit: Once again, Ford wants to sell people its new all-electric F-150. But:

1. Newspapers and magazines are basically gone as paper products – everybody goes to their websites now.
2. Radio is dead, as most people listen to streaming or podcasts.
3. Even TV is shaky, as young people mostly watch video on YouTube, TikTok, Instagram Reels, SnapChat, etc.
4. And there are at least **31 other content platforms now all competing for the public's attention** – console video games on Xbox/Playstation, games on phones, social media, online video, mobile video, mobile apps, etc. etc. - https://www.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/summary.html

It's too much for a car company to keep track of. Their business is making cars, not tracking tech content-consumption trends.

So **Ford turns to a specialized digital ad agency** and says, "We need a 360-degree campaign – one that hits our buyers no matter where they are. Watching TV, playing games, sharing social media posts, whatever."

Agency: "Oooh. That's a lot. **That'll cost ya.** But the good news is that with ad targeting, we can make sure that only people who are in the market for a car see your ad. We're snipers, not using shotguns like the Bad Old Days."

Ford: "Great! Here's $150 million for this quarter. Now get it done!"

The agency then goes to what are called DSP (Demand-Side Platforms), and says, "Hey, I want to buy ads for this new truck. But I only want them shown to people who are in the market to buy a new truck, or who bought a truck in the past, and who we might convince to upgrade."

Side note: A DSP is basically a marketplace for ads. Run by Google, Amazon, Yahoo, Facebook, TikTok, etc. https://skydeo.com/the-top-20-dsps/ It's a place where advertisers go to buy ads that are (supposedly) targeted to reach the audience most likely to respond.

Ad Agency to DSP: OK, I got $80 million ($150MM minus 20% agency commission, minus a bunch of Super Bowl ads at $3MM/minute to spend to buy ads to put in front of people who want to buy a F-150 pickup truck.

(Side note: Do agencies really take that big a slice of the ad spend? That's billions just for buying ads that the advertiser probably could have done on their own, right? Read it and weep: https://www.multicultural-marketing-agency.com/what-percentage-do-ad-agencies-take)

DSP: No problem. I've got all this data that shows exactly who is going to buy a truck in the next year. We can show them all the video ads you want!

Ad Agency: OK, but, um. A lot of the younger guys don't even watch TV any more.

DSP: Still no problem. We've got relationships with all the big video-game makers, phone companies, social platforms, websites – once we start spreading your ads, your customers won't be able to turn around without seeing a video of the new F-150 hitting them in the face.

Ad Agency: Perfect! Make it happen.

DEMAND-SIDE PLATFORM: LIKE EBAY FOR ADVERTISING

This is where it gets really REALLY complex. I'll try to make it as simple as possible, and in so doing, there will be areas where the analogies I use are not exact fits. Bear with me.

The DSPs have relationships with SSPs (Supply-Side Platforms). That is, companies that own websites, or apps, or games, or have video-streaming content where they want ad revenue.

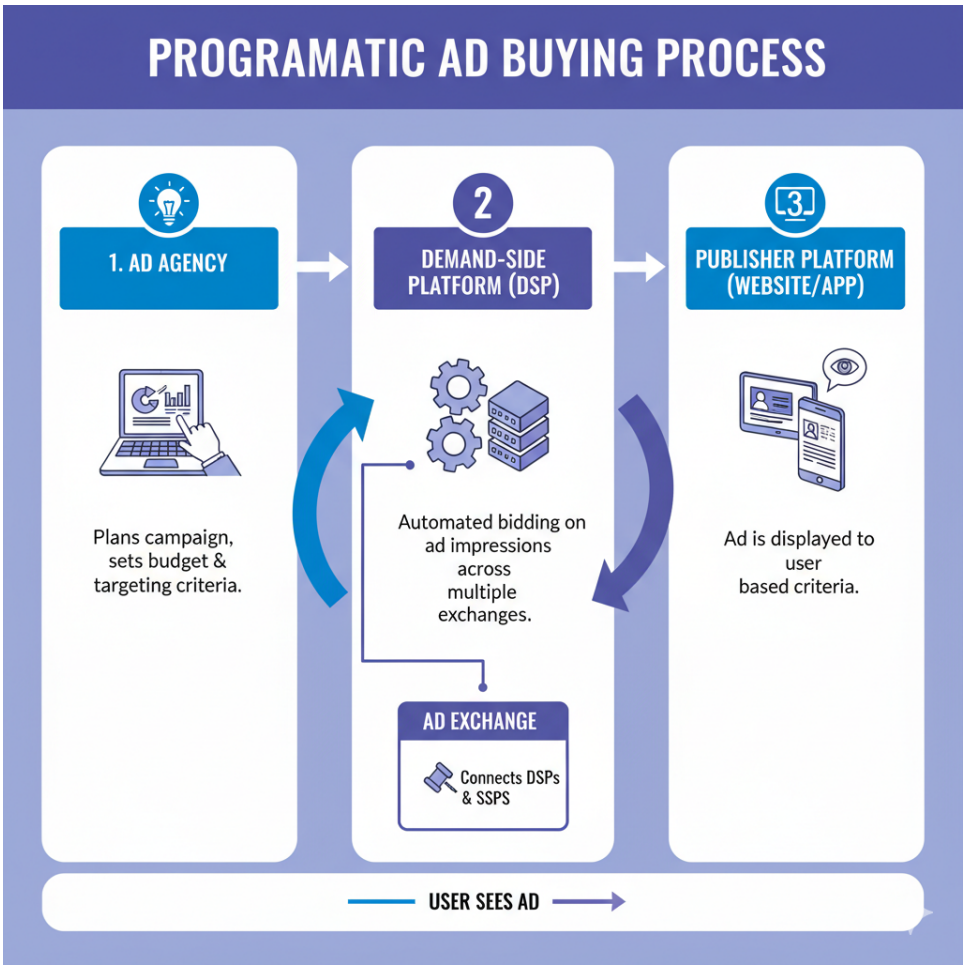
SSPs sell "inventory," or space on the sites/apps/games where ads can appear.

SSPs: "Hey! I've got a video that all my users are gonna watch. You can put 3 ads up front that they can't skip, 6 in the middle that will annoy the shit out of them, so you can really piss them off if you split into 2 segments of 3 each, and 3 at the end, just before the big climax."

DSPs: "Cool. But I want to buy ads not just for everyone, but just for people who fit these criteria (male, 18-49, bought a truck in the past, lives in rural area, makes $60K+/year, etc.)"

SSP: "Done. But that kind of targeting is going to cost you a premium. Normally the ads are $1.25, but for this, I'm going to charge $42."

This is how the process is supposed to work (note: I'm working on the graphic here – bear with me):



HOW IT ALL GOES WRONG

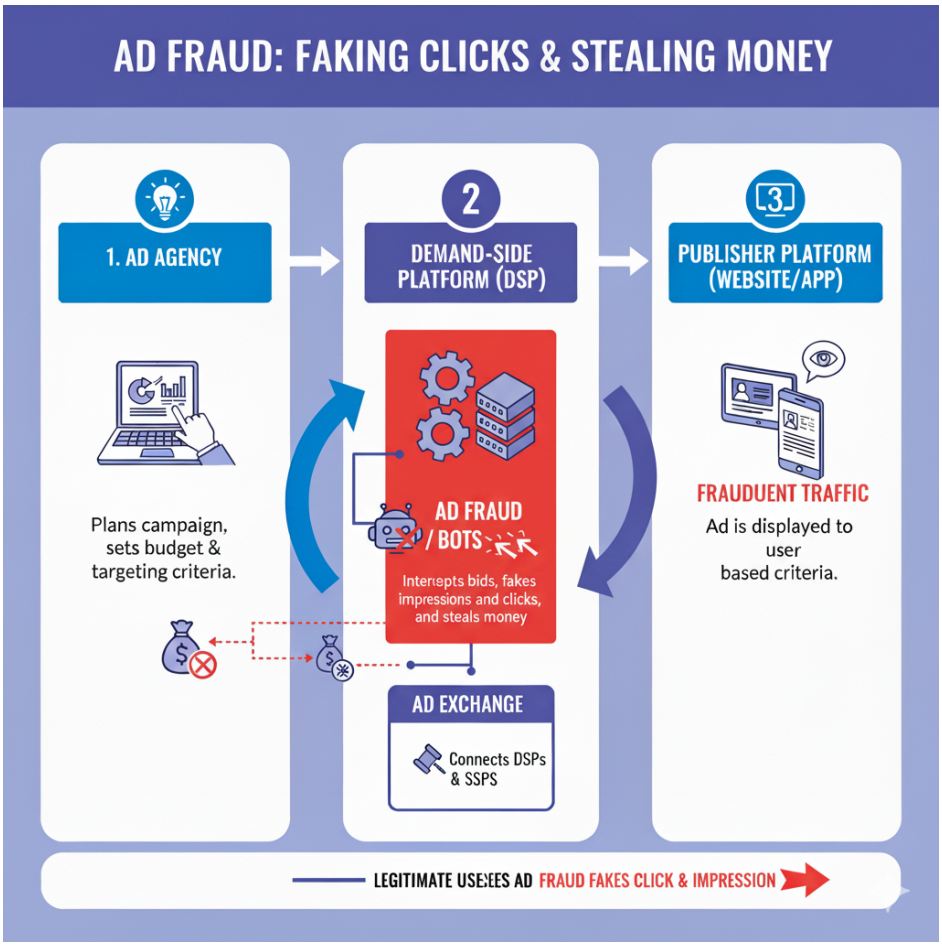
Bad Guys have built all kinds of MFA (Made For Advertising) sites that are just a janky URL and some content scraped from other sites around the internet. **These trash sites now represent about 20% of all websites on the entire internet.** Source: https://www.multiview.com/marketing/blog/the-rise-of-mfa-sites-and-what-advertisers-can-do-about-it

MFA sites use techniques like "ad stacking" and "pixel stuffing" to cram as many ads per page as possible. Most sites only show 3 or 4 ads per page.

An MFA site will "layer" ads, one on top of another, so that each page has 100, 300, or even 10,000 ads per page. In some sophisticated cases, **there aren't even spaces for the ads to appear – just "calls" to the DSP to serve the ad, which then triggers a payment to the Bad Guys.**

The MFA site owners go to the DSPs and say, "Hey! I've got a site that has all kinds of traffic, from people who are EXACTLY what you are looking for! Put some of those high-value ads on my site!"

The DSP and Ad Agency are mostly concerned right now with placing all the ads, so as to "get rid of the spend." Because unless and until they can burn through the money that Ford just gave them … **Ford won't give them money next quarter if they haven't spent the money THIS quarter.**



So neither the DSP nor the Ad Agency is particularly concerned about WHERE those ads are going. So the ads start getting sent to the MFA site(s).

On the MFA sites, **armies of bots are deployed to click over and over on the page and on the ads.** Each time there is a pageview, the DSP registers an "ad impression" and charges the ad agency for the ad placement.

This happens millions of times per second.

Now then. It's not all fraud. There are SOME legit ads being sent to SOME legit apps, games and sites. These are seen by real people, who then go to the Ford dealership and check out the new F-150.

But **about 20-30% of the clicks on the ads are on the MFA sites by bots.**

At the end of the month, the DSP sends a check to the owner of the MFA site for all the ad impressions the MFA site "delivered" for all the various ad campaigns.

None of these digital ads on the MFA site were ever seen by a human. The data & analytics for the campaign are kinda weird, but by now most people are used to a certain amount of weirdness in the system.

BONUS VIDEO: Dr. Fou explains **how the plummeting ad revenues and "scammer blindness" caused publishers to "turn to the Dark Side"** and push out all manner of ugly tricks to keep users clicking (like slideshows, carousels, and auto-playing video ads that take over your screen): https://youtu.be/Ad6KBqrGsB8

WHY AD FRAUD CONTINUES

Now that we understand the HOW … the question of WHY becomes more urgent. As in "Why does this continue? Why do advertisers keep paying for ads that aren't shown to humans? Why doesn't someone DO something about this?"

It's because **the remedies (so far) have been mostly aimed at the "buy" side of the equation.**

Which makes sense – at least on the surface. I mean, if you saw a friend buying an expensive new TV, but you happen to know it's just a hollow piece of plastic stuffed with lawn trimmings … yeah, you'd try to stop them, right?

But here's the thing: the incentives on the "buy" side run TOTALLY AGAINST fixing this situation. Why?

Well, imagine you're a big ad agency. Your data guys come to you with a big report: "Boss! We just figured out that 50% of the ad clicks we got in the last campaign for Adidas were total bullshit! It was fraud!"

What do you do with that information?

1. **Choice no. 1:** Call up the Adidas and tell them that 50% of their ad spend that they trusted you with was stolen
    a. Great. What is likely to be Adidas' response to this?
        i. "Good job finding the fraud. No biggie. Happens to everyone. Here's another $50 million. We trust you."
        ii. -OR-
        iii. "You jackasses! We want at LEAST $25 million back. And here's a lawsuit for all the lost sales we didn't get because of your malfeasance."
            1. Your ad agency's name is mud in the marketplace
            2. Even if anyone is stupid enough to trust you EVER, you will only be getting 50% of the ad budgets you got previously, meaning your commission just got cut by 50%. Genius move. See you in bankruptcy court.

2. **Choice no. 2:** Bury the report, fire the data analysts (signing them to draconian NDAs) and
    a. Pretend like nothing is wrong.
    b. Keep stacking the money.
    c. Blame "bad creative" if the Adidas campaign underperforms.

Guess which choice is the easiest.

WAIT – BUT DON'T ADVERTISERS CHECK IF THEIR ADS WORK?

OK, now we're really getting into the nitty-gritty of how ad fraud has gotten super-sophisticated. It's called **"Attribution Fraud," and it has grown & metastasized** over the past few decades, because the incentives are so huge.

In a nutshell: the scammers figured out that to run their ad fraud networks, they were going to have to figure out a way to game the system, **to make it look like the fake ads were delivering real results.**

The techniques include (*but are not limited to*):

- **Faked UTM sources** (putting "utm_source=XXX" where the XXX is a real high-value site like nytimes or msn or cnn, etc.)
- **Faking clicks on the [x] (ie the "Close" button** when users try to close an auto-playing video actually loads the scammers' sites with all the ad scripts firing immediately)
- **Writing fake data into Google Analytics** using a Python script on a server
- **Cookie stuffing** (aka "Cookie dropping") https://spideraf.com/articles/common-methods-of-cookie-stuffing-fraud
- **Click injection where malware on a mobile app** generates a fraudulent click on ads as users install an app (usually a "free" game or some such) https://www.cleartrust.cc/blog/what-is-click-injection-sneaky-mobile-app-fraud
- **View-through hijacking** where ads down below the top of the page drop tons of cookies and then take credit for showing the ads, even when they are never seen https://en.wikipedia.org/wiki/View-through_rate
- **Fingerprint spoofing** where fraudsters pretend to be you (or any other user) by collecting the data that identifies your brower/computer/phone and then using that to click on millions (billions?) of ads https://www.browsercat.com/post/browser-fingerprint-spoofing-explained

The details on how these are done are pretty tech-heavy, but if you are interested, there are many more resources available if you search for them, that talk about how these scams are done – and how most ad-verification services don't detect them.

See also: "Welcome to Ad Land: Where Clicks Are Made Up and the Numbers Don't Matter"

BOTTOM LINE: IT TAKES A HUMAN DIVING INTO THE ANALYTICS TO START TO DETECT THE ANOMALIES IN AN AD CAMPAIGN THAT OTHERWISE HIDE IN THE TOP-LEVEL NUMBERS THAT MOST PEOPLE JUST GLANCE AT.

Example: When the average is that the ads appear on sites with a 30% bounce rate and 1 minute time spent on the page … but it takes drilling down, site by site, to realize that **most of the sites have a 100% bounce rate from "users "that spend less than a second on the page before clicking away to somewhere else** (aka a bot), while the ones with human traffic have a very

low bounce rate and lots of time spent.

China's Fake Click Farm Is Massive: 4,600 Phones Operating, 8 Million Views, Only 100,000 Real

You can also watch this video about how Chinese fake "clickfarms" yank the motherboards out of phones, assemble them onto giant racks, and then use them to generate traffic on sites

https://youtube.com/shorts/-J7QvlzlFCo?si=O5ZbRf7ZnfKFROVq

It's even being reported on by Chinese media (screencap above):
https://www.youtube.com/watch?v=LFt0rkjQwkg

A SOLUTION. MAYBE?

First off, please know that I recognize that this problem is decades in the making, and billions of dollars large. Whatever resolves this dysfunction is going to need a massive effort by thousands of committed people, because the weight on the other side of the balance scales is a mix of corporate inertia, blind greed, and conniving thieves.

Right now – the best solution seems to be spreading the word about ad fraud, and trying to recruit more publishers into presenting a unified front to the massive tech giants that are monopolizing the global ad market.

Why?

Well, on the ad side, the incentives all run the other way. All the money is over on that side too.

Publishers and content creators are the ones getting ripped off – although look how it took me about 9 pages to try to explain WTF exactly is happening, why, and how come this problem persists.

If you've got other ideas on how to solve this imbalance, please feel free to reach out to me, and I will listen.

Well, unless your solution somehow involves blockchain and Web3 re-architecting the entire internet, because that wave crested and receded.