THE ECONOMIC COST OF BAD ACTORS ON THE INTERNET

AD FRAUD 2020

UNIVERSITY OF BALTIMORE

CHEQ

BAD ACTORS ON THE INTERNET

The internet has heralded an economic revolution. The internet economy of the G20 countries alone is worth more than $4.2 trillion representing 5.3% of their total GDP. However, as Tim Berners Lee, the father of the internet has put it: "While the web has created opportunity, given marginalized groups a voice, and made our daily lives easier, it has also created opportunity for scammers, given a voice to those who spread hatred, and made all kinds of crime easier to commit."

In a series of reports, we reveal the monetary cost caused by bad actors on the internet. CHEQ has worked with the economist, Professor Roberto Cavazos at the University of Baltimore, to undertake the first ever in-depth economic analysis of the full scale of internet harm. For the first time, using economic analysis, statistical & data analysis, we measure the global economic price paid by businesses and society due to problems including ad fraud, online bullying, and fake news.

AD FRAUD IN 2020: UNCOVERING A $35 BILLION PROBLEM

In this report, we focus on ad fraud—the practice of fraudulently representing online advertising impressions, clicks, conversion or data events in order to generate revenue. Digital ad revenue provides much of the financial underpinning of e-commerce and online-based businesses. Marketers suffer when their analytics tools report a substantial amount of web traffic, but the amount of revenue does not support the number of visitors tracked by their systems.

This problem has grown as digital ad spending has vastly surpassed traditional ad spending. In the following pages, we reveal that online ad fraud will cost advertisers $35 billion in 2020. This is a rise from the previous year, reflecting a surge of more sophisticated attacks, heightened further during the climate of COVID-19. The rise in ad fraud comes despite a contraction of digital ad spending. Further, indirect economic and social costs may increase the total cost, closer to $40 billion.
In addition to the direct costs, online fraud imposes indirect costs in the form of less trust, lost ROI from advertising spend and disinclination by some business to advertise online, and associated court costs which have risen to prosecute ad fraudsters.

In addition, the complexity at play, size and growth of digital advertising and asymmetric information within the advertising ecosystem has contributed to the rapid rise of the problem. There has been ongoing industry efforts and court enforcement, but as a study published in March 2020 showed, 15% of advertiser spend – around one third of supply chain costs – is completely unattributable.[1] This opacity remains a breeding ground for fraud, and while many industry actions are underway, the situation is certainly no better and only likely to face more challenges in the near and long term.

Professor Roberto Cavazos

University of Baltimore

Professor Roberto Cavazos, Executive in Residence at the Merrick School of Business at the University of Baltimore, has over 25 years' experience in economic analysis, statistical & data analysis, project and program management and policy, and technology with extensive experience in financial, data and health care fraud analytics and analysis for government and private sector organizations. He is also director of the risk and cybersecurity management program at the University of Baltimore.

[1] ISBA/PWC Programmatic Supply Chain Transparency Study (2020)

AD FRAUD ENABLED BY COMPLEXITY

Online advertising is a complex ecosystem and as such has become the target of abuse for botnets and other techniques used to defraud advertisers.
With increased complexity in any activity comes an increased probability of fraud. Likelihood of fraud increases with the number of participants in a complex system, and few sectors attract as many players engaged in a complex transaction as online advertising. Even in a simplified narrative of the process of placing an online advert, we see at least 23 categories of different player in this transaction (image via Luma Partners, 2019).

COMPARISONS WITH OTHER FRAUD-FUELLED SECTORS

Sector	Size of Sector	Fraud in Billons of Dollars	Percent of Fraudulent Activity
Digital Advertising	$333 billion	$35 billion	10.5%
Credit Card	$3.32 trillion	$27 billion	.008%
Insurance	$5 trillion	$80 billion	.016%
Health Care	$7.6 trillion	$456 billion	6%

AD FRAUD OVERTAKES CREDIT CARD FRAUD

This year, the losses from digital advertising fraud ($35 billion) have swiftly overtaken global annual credit card fraud ($27 billion). Despite the relatively insignificant digital advertising sector annual spend ($333 billion) compared to the $3.32 trillion credit card sector. The fraud rate in digital advertising is more than six-times higher than the insurance sector, 1.8 times higher than in health care and 13 times higher than the credit card industry.

This again is a factor of complexity and opacity which acts as a breeding ground for fraud, and digital advertising in particiular.

The Association of Certified Fraud Examiners cites increasingly complex transactions as a prime source of fraud in financial and investment markets.[2] In the U.S., complexity is one of the principal reasons why in 2014 it is estimated that Medicaid made $17 billion in improper and or fraudulent payments.[3] In the words of PJ O'Rourke, H. L. Mencken Research Fellow at the libertarian Cato Institute: "There is a simple rule here, a rule of legislation, a rule of business, a rule of life: beyond a certain point, complexity is fraud."

[2] https://www.acfe.com/financial-transactions-and-fraud-schemes.aspx

[3] 2MEDICAID: Key Issues Facing the Program GAO-15-677: Published: Jul 30, 2015. Publicly Released: Jul 30, 2015

However, fraud in the advertising sector stands out as more complex than other "fraud-fueled" industries. Compared to other sectors, online advertising is less regulated and less interconnected. Online advertising has created a situation in which the situation and interests of more than 20 parties are not aligned. In addition, there is little to disincentivize fraudsters. Indeed, a 2020 ISBA/PwC study, involving brands including HSBC, Walt Disney, and Unilever (each brand advertiser with 300 distinct supply chains), found that 15% of advertiser spend is completely unattributable. It notes that the data captured from a demand side platform (DSP) for an impression is not equally captured on the sell side. Impression matching cannot easily be performed at campaign level due to mission information in datasets. Independent ad fraud investigator, Augustine Fou, notes that complexity and lack of transparency is evident in reporting fraud levels. Fou notes that one party claims that invalid traffic (bots) is 10% on a campaign…while another vendor claims IVT is 1% on the same campaign. Sometimes the same vendors measuring the same campaigns (on behalf of the marketer versus on behalf of the publisher) shows different invalid traffic numbers."

Compare this lack of transparency to the financial and medical insurance sectors. These sectors are heavily regulated (by multiple government agencies) and US health insurers at most deal with 5 or 6 heavily regulated entities. In these industries there is tight interconnection and accountability—the payer has much control and the interests of all involved are fairly aligned. Improper payments or missing funds are eventually detected. The requirements for fraud prevention in online advertising add to this complexity. With credit card fraud, banks have limited amounts of requests say 1 million a day to investigate, however in advertising fraud prevention solutions need to analyze 20,000 requests per second. The spend on fraud prevention and resources in online advertising is insignificant, with some larger banks using more than 1000 cybersecurity professionals to monitor dangers.

Calls for greater transparency within the digital ecosystem, in order to lessen ad fraud, will be shown to be moot as has been the case for other complex markets. Complex market structures do not tend to rapidly transform and at present instances of the several types of ad fraud are technologically enabled. Ultimately, the frauds are due to information asymmetry (when parties do not have access to the same information) generated and reinforced by complexity, lack of transparency and regulatory oversight.

[4] ISBA/PWC Programmatic Supply Chain Transparency Study (2020)

CALCULATING THE COSTS: ONLINE AD SPEND REACHES $333 BILLION IN 2020

In a tumultuous year for advertising, nevertheless the total market expenditure on online digital ads is set to reach $332.84 billion in 2020.[5] To get a true sense of this magnitude this is larger than the GDP of Malaysia and almost half the GDP of Saudi Arabia. Despite some pauses in advertising spend because of COVID-19, there is little change in the direction towards digital advertising representing the vast bulk of global advertising spend. It is huge, and as previously outlined, a complex market, that is very tempting to bad actors.

DIGITAL AD SPENDING WORLDWIDE

[5] https://www.emarketer.com/content/global-digital-ad-spending-update-q2-2020

PERFECT STORM FOR AD FRAUD

In 2020, we have seen a perfect storm for ad fraud, as bad actors have exploited disruption caused by the global pandemic; large political spend tends to be largely unaccountable; and sophistication by ad fraudsters has increased.

1. COVID-19

The scale and sophistication of ad fraud attacks have only increased during the period of COVID-19. Previous recessions show a direct correlation between a fall in economic output and a rise in fraud.[6] In particular publishers felt the brunt of malvertising attacks between April and June 2020– estimated to have lost about 9% of their pageviews as user sessions were hijacked. Click fraud (paid search) represents 14% of search and paid social clicks, while click fraud affecting small businesses, the engine of the global economy, rose by 21% across paid search campaigns during the period of lockdown.[7] OTT programmatic ad spend, susceptible to ad fraud attacks, increased as streaming services saw a resurgence during lockdown, with OTT fraud rates representing 17% of marketer spend.

Meanwhile affiliate marketing fraud, reached 9% of spend in the $15 billion global sector. Brands turned to affiliate/ performance-based marketing as providing greater "certainty" during a recession, while consumers have been drawn to promised rewards offered, increasing affiliate activity.

The bright spot is that the pandemic represents a chance to start again with first principles in digital advertising. COVID-19 has focused minds on achieving long-sought after efficiencies, seeking to eliminate wasted ad spend. Harmony Murphy, Head of Advertising UK at eBay says: "In the world of online advertising, it's now more important than ever for every single impression to be a valuable one – and as they get back on track, brands can't afford to waste spend by serving ads to audiences that won't be interested in them."

[6] See for instance, Mark Button, director of the Centre for Counter Fraud Studies at the University of Portsmouth findings that during the 1990-91 slowdown, with a 1.7 per cent fall in GDP, involved a 9.9 per cent increase in fraud. The global financial crisis that began in 2008 featured a 2.1 per cent fall in GDP and 7.3 per cent rise in fraud.

[7] Merkle Digital Marketing Report, Q2 2020 found that despite COVID-19, search spend rose 9% Y/Y in Q22 2020,

2. DIGITAL POLITICAL SPEND

Though high profile big-spending digital events, notably the Olympics, were cancelled in 2020, digital political campaign spending in the US is set to reach $1.3 billion. This is particularly vulnerable to ad fraud. Zach Edwards, who worked on the online digital campaigns for President Obama and Mayor Bloomberg, says that up to 10-30% of a political campaign budget is wasted on ad fraud. He says: "There is no ad fraud department in most of these buying teams that can be spending "$30,000 to 50,000 a day" on political ads.

He adds: "There is a huge difference between political ad buys and business ad buys. In a business ad buy you have an ROI, you have people checking it for months afterwards, and if it didn't pan out you may ask for a refund, whereas in political buying the only day that matters is election day. So, you are spending money as fast as you possibly can. Because the political campaigns are so short, there is no accountability for ad fraud. But because the campaigns dissolve, no one ever checks that, and no-one ever asks for refunds."

3. INCREASED SOPHISTICATION

The sophistication of hackers attacking marketing spend has vastly increased. For the majority of fraudsters, the automation tools used to commit fraud are evolving without them having to do very much work – fraudsters just have to hide and rewrite certain elements in order to evade more and more tests. Bot-makers create millions of headless browsers, that can simulate all human-like actions such as mouse movement, page scrolling, and clicks, to load webpages and cause ad impressions which appear human. Malicious SDKs for advanced and AI-powered click injection are sold in the Dark Web to the public for a fairly low price to perpetrate ad fraud, offering the opportunity in the words of the suppliers to "emulate ad clicks and hijack clicks including Google, Facebook and organic clicks."

Meanwhile data center-dwelling bots have been replaced by fraudsters using harder-to-detect residential Windows systems running a Remote Desktop Protocol (RDP)[8] connection exposed to the Internet. This typically involves brute forcing million RDP servers all over the world.[9] The activity is from a real Window with an updated, valid Google Chrome browser. Unlike normal fraud schemes which are using bot/automation tools (Selenium, Puppeteer) in this this case, the attack uses a legitimate environment (for instance an updated Chrome, Windows, and residential IP).

Leading criminal lawyer Arkady Bukh, a New York-based attorney with a history of representing suspected hackers and ad fraud perpetrators from Eastern Europe, including those involved in the "Methbot" case,[10] says the growth in sophistication by bad actors is marked. "There is widespread fraud from huge amounts of traffic getting directed through botnets. Before, it was boys and girls in Russia sitting in boiler rooms clicking manual clicks in order to get apparent traffic to defraud affiliates. Now it's done by bots."

[8] RDP is a remote desktop protocol, providing a user with a graphical interface to connect to a different computer over a network connection. Although without controls it can be a significant security risk.

[9] See for example GoldBrute, the botnet searching for RDP connections https://www.pandasecurity.com/mediacenter/malware/goldbrute-botnet-rdp/

[10] The Methbot case is estimated to have cost marketers at least $3 million dollars each day the botnet operated

RATES OF FRAUD

The World Federation of Advertisers which represents 100 of the world's biggest brand owners and 60 national advertiser association is well placed to draw industry insights. They estimate, in line with many independent fraud experts, that 10 to 30% of advertising is not seen by consumers and thus spend for unseen ads is a direct cost due to ad fraud.[11] Even best case scenarios accepted by the industry, shows that 8 % of display advertising impressions are fraudulent, 14 percent of video ads are fraudulent[12]. Though some collated industry figures put ad fraud at around 2%, many ad verification companies do not detect sophisticated frauds (SIVT) which is both harder to detect and brings greater damage to the bottom line of businesses. Often surveys donwplay ad fraud levels in fast-growing digital advertising markets: for instance, ad fraud in India reaches as high as 39% in India, and 29% in Russia and 20% in Mexico. It should also be noted that some studies used to calculate the cost of global fraud are based on a limited sample of impressions. This sample in some cases amounts to analyzing a relatively tiny (27 billion impressions) of the 70 trillion ad impressions each year.

Moreover, it is a basic principle of fraud that instances will always be under-recorded. Even in the case of financial fraud (costing US corporations up to $364 billion annually) and subject to watchful regulators, it has been shown that for every fraud caught at least 1-2 additional frauds go undetected.[13]

This of course, concerns instances of financial fraud detection probed by well-funded bodies such as the SEC. By contrast, the online ad industry faces nothing close to this level of scrutiny, such that probes have been launched in the past year by the UK and Australian governments to better understand the online advertising ecosystem among governments and regulators.

Undoubtedly the incentives for fraud remain much larger than almost any other industry. There are minimal court cages against offenders who remain incentivized by high payoffs.
Of course, many fraud attempts are invalidated by demand-side platforms (DSPs) or supply-side platforms (SSPs), before being paid for, but the sophistication of attacks means that the rate of attacks are constantly keeping pace with fraud detection efforts.

[11] See: https://www.wfanet.org/

[12] Business Wire, May 1, 2019, Report from ANA and White Ops Shows War on Ad Fraud is Succeeding

[13] See 2017: How Pervasive is Corporate Fraud? Alexander Dyck (University of Toronto); Adair Morse (University of California at Berkeley); and Luigi Zingales (University of Chicago)

THE DIRECT COST OF AD FRAUD

If we assume the different rates of fraud noted by industry experts as a percentage of digital advertising spend, we see the magnitude of the problem. Using the World Federation of Advertisers' assessment of ads not seen by intended audiences we note that between 10% and 30% of ads are not seen. Rates of ad fraud vary by channel. This is around 9% in affiliate marketing spend, 14% in paid search and paid social; 14% in mobile apps; 17% in OTT spend; and up to 30% in display. However, tempting to assume that 9% to 30% of ads not seen translates to 9% to 30% of ad fraud it should be noted that not all unseen ads cost the same.

Our experience suggests that higher end campaigns through well-known reputable advertisers are subject to a 5%-10% fraud rate, whereas lower-end campaigns experience a much higher rate of ad fraud potentially up to 50% (though they are a much smaller portion of total ad market). Thus, businesses using lower cost advertising services or gaining cheap traffic are more likely to suffer from advertising fraud.

Industry insiders' insights suggest that a 10.5% composite rate of total ad spend lost to ad fraud reflects the mix of lower end and higher end ad campaigns for a total annual loss of $35 billion estimated for 2020. Left unchecked the direct level of fraud is expected to reach $41 billion in 2021 and $46 billion by 2021.

Though all types of digital advertising face fraud, now we analyze fraud trends in the main digital channels.

DISPLAY

Programmatic advertising is the economic fuel of the "free" internet and in the US alone marketers will spend $68 billion a year on programmatic display. Its rise has made it dramatically easier for anyone to create their own site and immediately make money from traffic. Unfortunately, the same convenience that allows a food blogger to turn their following into an income also allows anyone to set up a site pushing hate speech or propaganda and get it monetized without any advertiser explicitly choosing to pay them.[14] Duane Brown, Founder and Head of Strategy at Take Some Risks, says: "We don't tend to do much on display as it is pretty trash traffic. I am sure we have ads and videos that appear on sites we don't want them to appear on, but we take what precautions we can."

MOBILE APPS

At least $4.8 billion is lost by marketers to mobile app ad fraud. Fraudsters are naturally attracted to a combination of high volume and high payout, putting the finance and shopping verticals at the greatest immediate risk. To highlight the problem for instance, Union Bank, the Philippines tenth-largest bank, in a race to fast-track user acquisition for its UnionBank Online app, found levels of fraudulent installs approaching 88% among their media partners. Install hijacking, click flooding and device emulators (a tool used by fraudsters for various bot-related fraud schemes or large-scale device farm operations) are frequently detected.

Fraud in this sphere may see fraudsters plant malware-laced ads on users' phones or embedding malware in apps and online services to generate clicks fraudulently to receive payouts by advertising networks. The Google Play Store has had regular attacks from fraudsters. In February 2020, apps, (mostly camera utilities and children's games)were laced with a malware strain dubbed Haken, stealing data and signing victims up for expensive premium services.

In February, announcing the banning of 100 apps from the Google Play Store, Per Bjorke, Senior Product Manager, Ad Traffic Quality at Google confirmed the scale of the problem: "Mobile ad fraud is an industry-wide challenge that can appear in many different forms with a variety of methods, and it has the potential to harm users, advertisers and publishers." In March, the Google Play store also removed 50 Android apps compromised by the Tekya auto-clicker-malware. In June 2020, popular barcode apps producing ads that instantly vanish were removed after being downloaded 1 million times. In April, 29 apps were identified and removed, but had collected 3.5 million total downloads. Such app frauds include the sneaky serving of ads, calling up fake browser pages outside the user's control, and ads displayed while phones are unlocked or charging.

User reviews of such apps begin with bot-driven five-star reviews. This is followed by genuine human reviews confirming that such apps are barely functional.

[14] Gilad Edelman, Wired, 28 July 2020: Follow the Money: How Digital Ads Subsidize the Worst of the Web

PAID SEARCH AND PAID SOCIAL

Paid search spending, according to industry estimates, will grow over the next couple of years. This channel will see 5% growth in paid search advertising this year, followed by 13% in 2021. Based on empirical-based research, we found that 14% of PPC spending is invalid across paid search and paid social based on platforms attracting PPC dollars, including Google, Facebook, Bing, Yahoo, Baidu, Snap, Twitter, LinkedIn, and Amazon. Click fraud is driven by many different sources, from standard web crawlers, to malicious bots, click farms, ad-fraud schemes and even competitor clicks, fake accounts, data centers, and the challenges of Facebook's Audience Network. The highest sector for loss in paid search and paid social includes, eCommerce sites (set to lose $3.8 billion to click fraud in 2020); followed by travel ($2.6 billion) and education spending ($830 million).

PUBLISHERS

Publishers have faced severe economic challenges from ad fraud. This is on top of brand safety economic pressures, emphasized in a separate report in this series. For instance, Newsweek launched an investigation and was forced to issue a news release, after it was "alerted to a piece of potential code that disrupted ad tracking and ad viewability". The Indian edition of the International Business Times has been caught three times using deceptive ad practices to inflate views, blamed on a "rogue employee". Showing the economic incentives of such fraud, the publication said the employee sought to " boost his performance metrics…[employing] shortcut methods to reach monthly targets".[15]

In one investigation, Megan Graham, a CNBC reporter showed the ease of setting up an illegitimate news website and monetizing it with online ads. The fake site attracted ads from top brands including Kohl's, Wayfair, Overstock and Chewy". [In a statement, Overstock said that as an advertiser it is negatively impacted by this fraud and does "everything in [its] power to prevent it."] It has been estimated that such fake news site can make $100,000 a month from inflating traffic with bots, and attracting online ads. UK brand, Virgin Media, one of dozens of brands advertising on such sites, said: "We hope more can be done across the industry to clamp down on these instances of pay-per-con advertising fraud."

Even when affirmative action has been taken where brands sought to prevent their ads appearing on Breitbart, so called "dark pooling" (sharing of ads.txt identification) effectively mislabeled inventory and funneled ad dollars back to such sites.

The Financial Times was hit by domain spoofing of its trusted brand, with the publisher estimating the value of a fraudulent inventory, across 10 ad exchanges to be $1.3 million a month. Decrying the incident, Anthony Hitchings, the FT's digital advertising operations director said: "The scale of the fraud we found is jaw-dropping. The industry continues to waste marketing budgets on what is essentially organized crime."

In setting out its views on the market problems of online advertising, the UK's competition watchdog, the Competition Markets Authority wrote in July 2020: "If problems in the digital advertising market mean that [publishers] receive a lower share of advertising revenues than they should, this is likely to reduce their incentives and ability to invest in news and other online content, to the detriment of those who use and value such content and to broader society."[16]

[15] IBT India's site used a combination of methods, including bot-like behavior on its pages, to artificially increase the number of pages and ads being loaded.

[16] https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#interim-report

OTT FRAUD

Marketers are expected to lose $4 billion in 2020 due to OTT ad fraud, according to our estimates. Over-the-top (OTT) media services are streaming media services offered directly to viewers via the Internet. Brands are projected to spend $23.8 billion in 2020 to show ads on connected devices, like Roku, and over-the-top media services, which are streaming platforms like Hulu. Advertisers increasingly invest in fast-growing ad-supported streaming platforms globally. However, at least a quarter of that money will be stolen by fraudsters, according to almost all ad fraud services and experts.

The industry has seen a 232% rise in the number of OTT apps supporting programmatic, while during lockdown, total hours spent with CTV devices were up 81%, equating to nearly 4 billion hours of CTV use per week. With smart TVs and other connected TV devices enjoying higher CPMs, the fraud focused on on spoofing these two types of devices. OTT ad fraud cases brought to light in the past year include the so-called IceBucket botnet in which fraudsters discovered weaknesses in the SSAI server communications mechanism

In another case involving Grindr (January 2020) "ad spoofing" saw cheap banner ads used to resell more expensive video ads. In another case (March 2020) an alleged ad fraud scheme ran on Roku, was said to cost "seven figures". Marketers from brands including Jaguar, Geico, and Lexus, had purchased what they believed to be ad space alongside popular content; however, it emerged that these brands' ads were being displayed in spots alongside screensaver and pet entertainment apps, and not to the viewers they had hoped to reach.

Joe Barone, managing partner for brand safety in the Americas at GroupM, the world's largest media investment company responsible for more than $50B in annual media investment, said of the rise of OTT ad fraud: "Right now, we're looking at a big bucket of invalid traffic. It's not just fraud. There's content that's emanating from outside of U.S., redirects to user-generated content, and straight fraud like spoofing. … There are a number of different things adding up to [problems] we don't want to pay for."

[15] IBT India's site used a combination of methods, including bot-like behavior on its pages, to artificially increase the number of pages and ads being loaded.

[16] https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#interim-report

OTHER AD FRAUD

Fake ads on social media platforms also hit brands including Patagonia, Microsoft, and Ralph Lauren. This involves leveraging Facebook's powerful advertising tools to target people with fake promotions for products, and then directing them to other websites siphoning credit card details or selling counterfeit versions of premium brand products. Between February and July, Patagonia says it received more than 1,500 reports of fake Facebook ads for its products. In another variation of fraud techniques, in February, 2020, more than 500 browser extensions, downloaded more than 1.7 million times from Google's Chrome Web Store, were found complicit in ad fraud. In addition there have been cases of email-based extortion with bot-runners threatening to flood websites with fake traffic unless payment was made, at a cost of a $5000 to avoid this eventuality.

Through the sophistication and spread of ad fraud hitting multiple companies on a daily basis, we see the bottom-line impact on the wider economy. Indeed, our figure of $35 billion lost to ad fraud in 2020 could be even higher still if the indirect and opportunity costs of ad fraud are factored in.

INDIRECT AND OPPORTUNITY COSTS

We have found that the direct costs associated with ad fraud will reach at least $35 billion in 2020. However, there are intangible costs associated with ad fraud as well, which have not been factored into this estimate. The US government has suggested that to best understand the cost of crime, estimates should consider both the financial and non-monetary effects of harm—such as the impact on quality of life, increasing fear, or indirect effects, such as change in behavior.This has concluded that crime's most costly factors stem from these less tangible effects.[17]

Direct costs refer to the direct losses and damage as a result of the situation, while indirect costs are the losses and opportunity costs imposed on society by the fact that the fraud is carried out.

Some indirect costs of ad fraud may include less trust among actors and thus less innovation. Advertiser clients may over time become less inclined to spend. In the words of Per Bjorke, a senior product manager who leads Google's ad traffic quality team: "It's very simple. The future growth of Google and other companies hinges on the fact that online advertising is trusted, and that there will be a return on investment on ad budgets … It's very important for us because people could stop investing in advertisements."

ENFORCEMENT ACTIONS

Indirect costs also include expensive enforcement (see table of 2020 ad fraud court cases and enforcement actions, p.19). This encompasses significant time and executive investment in tackling these problems. Rob Tadlock, Patagonia's associate general counsel, said hunting down ad fraud, involving ads on networks disguised as their brand, requires ongoing major investment from its legal and customer service teams.

[17] United States Government Accountability Office: Experts Report Challenges Estimating Costs and Suggest Improvements to Better Inform Policy Decisions https://www.gao.gov/assets/700/691895.pdf

DAMAGE TO FUNNELS

There is also the damage done to marketing strategies driven by bots polluting data on ad campaigns. In many cases for instance retargeting spend is wasted chasing after bots that visited promotions. In the ongoing case of Las-Vegas based Online golf equipment retailer Motogolf.com (2020), the sports retailer sued TopShelf Golf, alleging they violated federal and state law by repeatedly clicking on Motogolf's pay-per-click online Google ads. According to the court complaint, beyond the immediate economic damage, the alleged victim is suffering from losing "valuable demographic data about prospective customers".

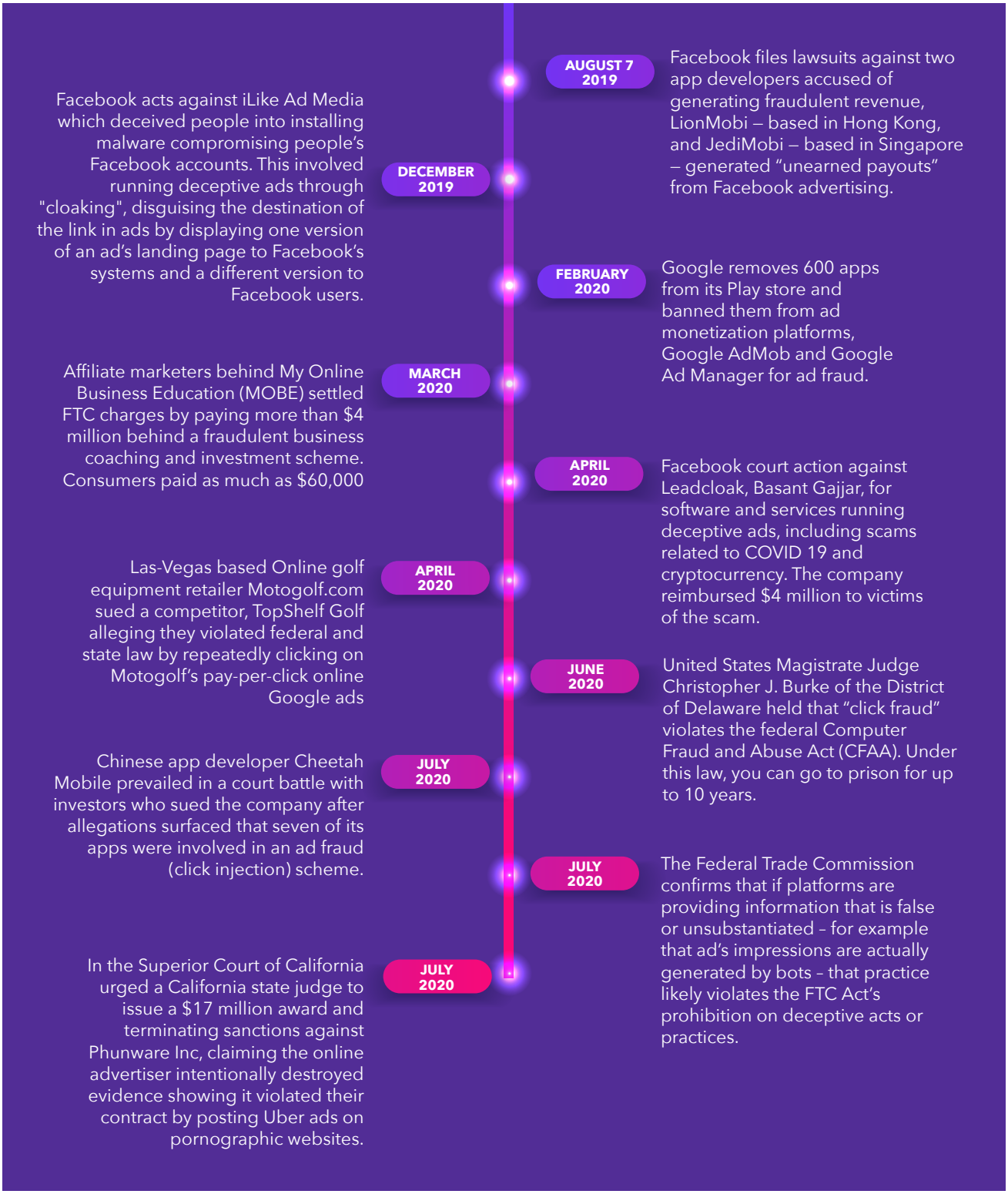
OPPORTUNITY COSTS

Lost economic opportunities in this area might be more difficult to measure because the calculation involves focusing on what might have been if fraud was not in play. Companies, however, should consider and even quantify the lost economic opportunities so a true picture of losses suffered can be determined.[18]
Lost budgets could have produced value for advertisers had they been wisely invested in other profitable channels. This is considered as the alternative cost. In an alternative scenario such digital campaigns could have converted more prospects and produced greater revenue for the business.

Indirect fraud damages are felt across all entities and players within the marketing ecosystem. For instance, a lack of fraud treatment could mean losing an ad network's reputation and risking its future business with leading advertisers, limiting their media portfolio in exchange for cleaner traffic. Moreover, legitimate networks often lose credit for quality users they provided due to attribution hijacking tactics, stealing their credit using fake clicks. The costs of such challenges, though representing a significant business burden, cannot be directly calculated.

[18] Association of Certified Fraud Examiners (2015) Measuring the economic impacts of fraud

RECENT AD FRAUD COURT CASES AND ENFORCEMENT



INDUSTRY ACTION

By 2020, the industry has recognized the challenges of ad fraud and ongoing efforts are being made to tackle the challenges. For instance, Google has deployed Play Protect as a means to screen potentially harmful applications and also forged an "App Defense Alliance" in partnership with cybersecurity firms to reduce the risk of app-based malware. The IAB Tech Lab partnered with the Advanced TV committee to craft the guidelines for improving measurement in SSAI and, more broadly, across OTT/CTV advertising. In February 2020, the industry watchdog, the Media Rating Council (MRC) also updated its guidance, in relation to a more sophisticated fraud ecosystem, covering new threats involving sophisticated invalid traffic, in-app, OTT and other rapidly emerging digital ad environments. In August 2020, the Trustworthy Accountability Group (TAG) issued best practice guidelines to combat the rise in malware.

CONCLUSION: THE RIGHT TIME TO TACKLE AD FRAUD

Fraud has a way of hiding in plain sight. In an entirely different sector, the $3.9 billion Wirecard scandal surfaced in 2020 (described as "the Enron of Germany"). This shows us that even in 2020 fraud not only exists but thrives at the highest level. In the world of digital advertising, marketers concur that online fraud remains a challenge. According to an ANA survey, more than 70 percent of advertisers consider invalid traffic and fraud in digital advertising" to be a top concern.[19]

The reasons fraud continues boil down to the systemic opacity and complexity of online advertising and the increase in motivation and resources to perpetrate fraud. It has also been pointed out that the ongoing prevalence of ad fraud is a byproduct of the fact that the average CMO tenure is getting shorter, and that marketing leaders may be focused on bigger, more visible wins. This would be a mistake in the current climate for any executive leadership team seeking to restore revenues through reaching real customers. Though COVID-19 brings an extra uncertainty to digital marketing, it should not be viewed as a reason to pause the fight against bad actors online. The need to account for every dollar and the motivation to restore revenues attracting more visitors and buyers through digital advertising means that the requirement to challenge of ad fraud is more pressing than ever.

[19] ANA/Reed Smith: September 2019: Trust Consortium, Issues that Contribute to the breakdown of Trust in the Advertising System

POSTSCRIPT

CHEQ

"Advertising needs to step up to its responsibility for its supply chain and the fact that it funds the internet, the good stuff and the bad stuff. There isn't a big investigation into ad fraud because I don't think enough people understand it, and certainly not in government. Regulation and legislation are miles behind the technology. It's a murky world."

Jake Dubbins
Managing Director of Media Bounty and co-chair of the Conscious Advertising Network

"When the numbers look good, no one is questioning them – and marketing fraud makes the numbers look good."

Angus McLean
Director, global marketing, Ebiquity

"If platforms are providing information that is false or unsubstantiated – for example, if many of an ad's impressions are actually generated by bots – that practice likely violates the FTC Act's prohibition on deceptive acts or practices. By challenging false claims, the FTC can better protect businesses that may be overpaying for ads."

Commissioner Rohit Chopra
Commissioner, Federal Trade Commission

"The concept of "FOFO" – fear of finding out – is one of the ironic truths in this space, describing the incentive misalignment on solving the issue. Fraudsters try to access marketing budgets by generating and selling invalid traffic, but all other parties may have conflicting interests."

Danilo Tauro
Global Director of media, tech and data, Procter & Gamble

"This is an industry that is constantly talking about wanting to transform itself, but that is also constantly sticking to very traditional approaches. Old habits die hard, but people are being forced out of necessity to adapt faster."

Marcelo Pasco
VP Marketing, Coors