THE ECONOMIC COST OF BAD ACTORS ON THE INTERNET

AFFILIATE MARKETING | 2020

UNIVERSITY OF BALTIMORE

CHEQ

THE ECONOMIC COST OF BAD ACTORS SERIES

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 commissioned 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.

AFFILIATE MARKETING AD FRAUD

CHEQ

UNCOVERING A $1.4 BILLION PROBLEM

In this report, we focus on the problem of online affiliate marketing, or "performance marketing". This performance-based approach to online marketing sees advertisers only pay when a sale occurs, involving online tracking that attributes sales to affiliates. Affiliates are third-party, independent websites, such as travel blogs, information pages and interest groups, who are willing to display advertisement links for a monetary gain.[1]

The problem occurs with bad actors exploiting shortcomings in tracking and attribution to claim commissions unfairly, damaging marketers and the bottom line of many businesses. In the following pages, we show that affiliate marketing fraud will cost advertisers $1.4 billion in 2020. Left unchecked, the problem will continue to grow with global expansion of affiliate marketing into new markets and countries, particularly as the appeal of affiliate marketing continues to grow in a downturn.

ECONOMIC COST OF AFFILIATE FRAUD

Marketers are expected to lose $1.4 billion to affiliate marketing fraud in 2020, based on the current size of the sector and rate of fraud. Our analysis is based on the level of fraud at a conservative level of 9% within the $15 billion affiliate sector. This analysis and uptick in fraud in affiliates comes at a time when reliable digital marketing spend is more crucial than ever to the success of enterprises in all sectors facing a significant downturn.

THE CHALLENGE OF AFFILIATE FRAUD

Affiliate marketing promised to remove many of the risks associated with traditional digital marketing channels. So-called Pay Per sale marketing was proclaimed by The Economist as the "holy grail of advertising" "liberating advertisers from the old cost-per-thousand model, in which they targeted audiences and then blindly threw money in their general direction." In contrast "Pay Per Sale "will liberate advertisers from all wasted spending by tying their costs to real sales".[2]

However, affiliate marketing has faced its share of fraud, and a renewal of fraudulent tactics as affiliate marketing continues to grow. In this context, affiliate fraud refers to any false or unscrupulous activity conducted to generate commissions from an affiliate marketing program. Affiliate fraud also encompasses any activities that are explicitly forbidden under the terms and conditions of an affiliate marketing program. This has been described as "the dark side" of affiliate marketing.

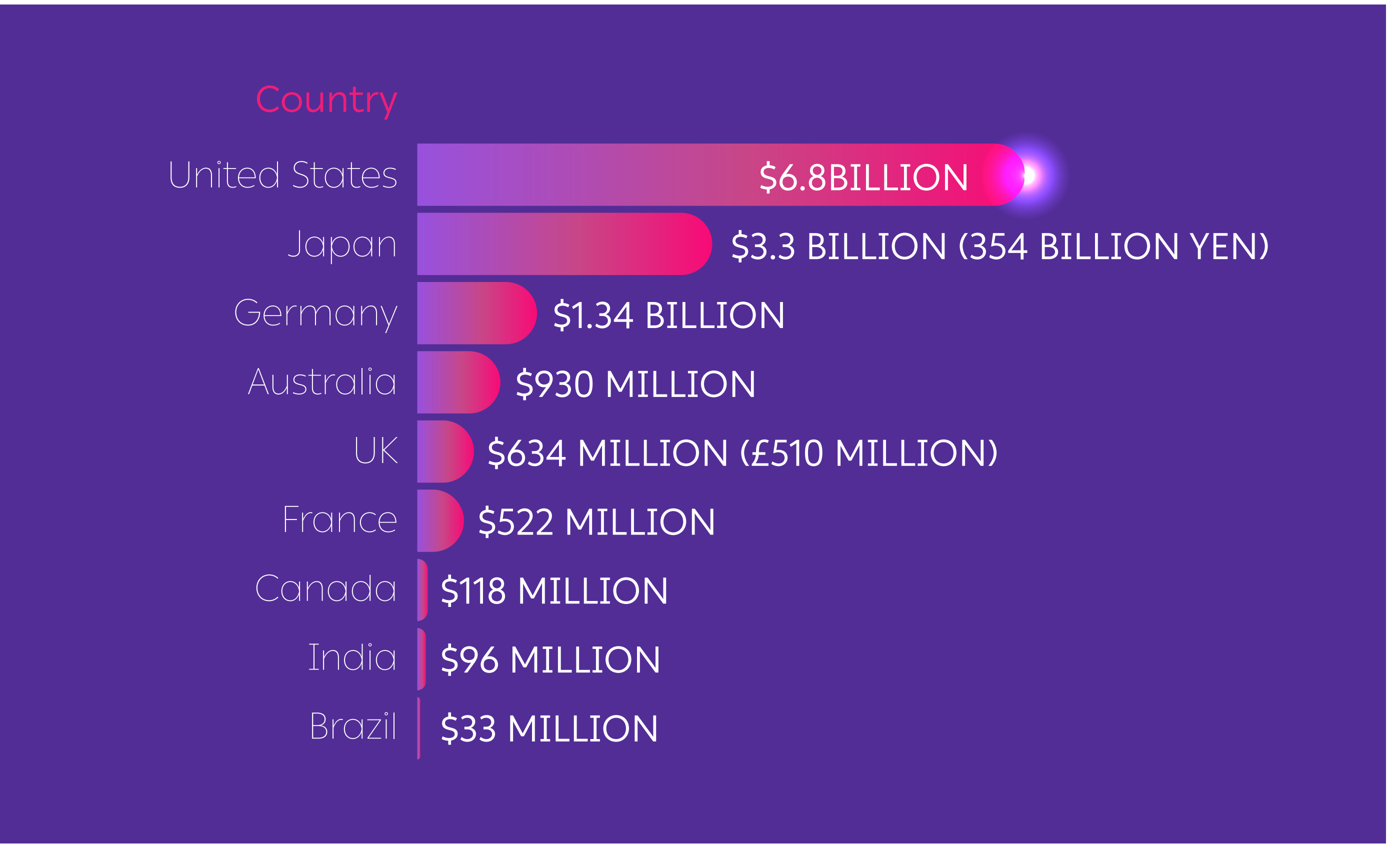
[1] Exploring Risk and Fraud Scenarios in Affiliate Marketing Technology from Advertiser's Perspective, Amareskara & Mathrani (2015)

[2] The Economist, Pay Per Sale (2005)

SIZE OF AFFILIATE MARKETING INDUSTRY GLOBALLY IN 2020: $15 BILLION

CHEQ

The size of the affiliate marketing industry continues to grow, and in 2020, we estimate the sector to be worth $15 billion.[3]



The largest market in the United States stands at $6.8 billion. Japan sees $3.3 billion in affiliate marketing with the domestic market growing 15% each year. In the UK $634 million (£510 million) has been poured into affiliate marketing programs. Germany's retail trade association Handelsverband Deutschland (HDE) estimates that mobile commerce sales alone in the country sees $1.34 billion from affiliate marketing. China's growing affiliate marketing industry demonstrate the size of the market. Rising affiliates such as Chanet work with more than 300,000 websites connecting affiliates focused on recruitment, education, travel, networking, entertainment, and e-commerce. Also, in China, YiquiFa, generates an average of 20 million clicks and 2.5 million sales per day; while LinkHaiTao works with foreign businesses including Nike and Rakuten. In Australia, almost a third of brands and agencies currently spend over 10% of their Marketing budgets on affiliate marketing.

[3] Based on independent analysis but consistent with Forrester Research (2017) showing a market value of $12 billion and calculating annual growth of 10%.

THE ECONOMICS OF AFFILIATE MARKETING

The majority of affiliate programs involve cost per action (CPA). This is a performance pricing model in which marketers pay media sources a fixed amount based on a pre-specified action. For instance in a study by the IAB of 70 marketers engaged in large scale affiliate marketing in Australia, found that it while almost all brands engaged with affiliate marketing use Cost Per Action (99%), a minority use Cost per click (19%), cost per lead (16%), and cost per thousand, known as CPM (used by 14% of programs).

Beyond affiliates and the payouts from the brands themselves, affiliate networks play a vital role in the ecosystem. Networks bring in new advertisers, track leads and send out payments. For performing this overhead, affiliate networks receive a commission, usually receiving 14-30% range for their work. Some of the biggest affiliate networks are Amazon Associates, eBay, Commission Junction, Rakuten Marketing Affiliate and Awin.

PAY PER SALE

It has been estimated that up to 15% of all digital media industry's revenue comes from affiliate marketing. For many companies, pay per sale, particularly in the travel and retail space affiliate marketing has become their lifeblood. Several brands are seeing 20% of their e-commerce revenues stemming from affiliate marketing, sometimes only mere months after launching their programs. It has extended to finance, loans and investments. For instance, eToro a social investment network has reportedly paid out $87 million in commissions to its affiliates since its inception. For Amazon 6% of its hefty 2.5 billion online visits a month arrive from affiliate sites.[4]
Indeed, in a typical cyber Monday, about 16% of sales comes from affiliate traffic.
This is drawn from 81% of advertisers that adopt affiliate marketing as part of their core marketing strategy, while, 84% of publishers adopt affiliate marketing.

[4] SimilarWeb data accessed June 2020

LARGE PRIZE FOR TOP AFFILIATES

CHEQ

For those being paid by affiliate programs there is substantial money to be made. High-profile affiliate leaders include Pat Flynn, Smart Passive Income, who made over $100,000 in a single month, or Zach Johnson, earning $100,000 every year. In the world of sports gambling, Shahbazyan generates 25-40% lifetime commissions on net gaming revenues from referrals creating $2 million per year.[5] The affiliate website—The Wirecutter—made an estimated $10 million in revenue, and was sold to the New York Times for $30 million. In policies on affiliate links, Wired, calls editorially independent affiliate links "another means of paying for the high-quality journalism you expect".

GROWTH OF THE AFFILIATE MARKET INDUSTRY POST COVID-19

During COVID more brands are turning to performance channels because advertisers only pay when they see success, in theory diminishing risks. In a period of "lockdown" from April 2020 affiliate volumes rose in many sectors: gifts and flowers rising 80%, computer and electronics up 66%, health and beauty rising rose 41% [the so-called "lipstick effect" of recessions][6] home and garden rose 28%, and sports and fitness, 6%.[7]

In addition, as brands cancel influencer-marketing campaigns or put projects on hold, affiliate revenue has become a growing source of income for some digital creators and those who are unemployed. At the same time publishers – countering a loss in advertising revenue, seeking alternative cash sources, are turning to affiliate marketing. Indeed leading affiliate network, Rakuten found that nearly half (42%) of affiliate publishers reported an increase in site traffic during the pandemic.

RATES OF FRAUD IN AFFILIATE MARKETING

The rates of fraud in affiliate marketing are highly debated. Indeed, it depends on the type of transaction – for instance up to 25% of app installs are considered to be fraudulent most often as a result of attribution fraud. Based on proprietary CHEQ data based on more than a trillion impressions, representing more than 39 sectors, and detailed interviews and insights from affiliate and marketing experts we consider the rate of fraud at 9% across affiliate marketing.

This is highly conservative estimate of fraud and many marketers report finding much larger percentages of fraud in their affiliate programs. Indeed, it was only four years ago that the University of Illinois estimated that 38.1% of partners in the Amazon affiliate program engaged in fraud.[8]

[5] Inc: How Sports Betting Affiliate Marketer Makes $2 Million Per Year

[6] Washington Post: The creative ways beauty pros are facing the pandemic, June 18 2020

[7] Media Post: Performance Marketing Gets A Lift As Advertisers Look For Guarantees May 12, 2020

[8] Journal of Cybersecurity: Characterizing fraud and its ramifications in affiliate marketing networks, Peter Snyder and Chris Kanich, University of Illinois at Chicago (July 2016)

RISE OF AFFILIATE MARKETING FRAUD

There have been major cases (see table) which show the significant costs of affiliate fraud on the bottom line of enterprise businesses. In one high-profile ongoing case ride-hailing company Uber says that it was duped out of more than $70 million through attribution fraud. Like most cases of affiliate marketing fraud this involved allegations of a scheme that credit affiliates for purchases from users already on the verge of making purchases. However, all digital sectors are affected from finance, to travel and tech. In one case in which CHEQ is investigating, a personal loans company is seeing a 9.6% fraud rate coming from their affiliate channels. Such affiliate fraud is triggering a large volume of "loan reverses". This sees the loan company approve loans based on a specified criterion, only then to cancel it as details turned out to be fake or fraudulent. This has seen affiliates place a massive exposure on the loan business which was forced to rip up loans of those likely default on their payments.

In another case, a major travel-tech platform, spends millions of dollars across multiple search and paid social channels. In this case, 22% of the client's incoming ad clicks were either completely fraudulent or invalid, with the vast majority of these clicks driven by the client's affiliates. This included fraudulent, non-human traffic from affiliate sites, email campaigns and referrers including travel agents and hotels, amounting to millions of dollars in wasted ad spend.

In the words of Ben Edelman, a researcher and professor at Harvard Business School, and now an economist at Microsoft, the profile of an affiliate fraudster "remains a white guy in the United States. I've got lots of stories about foreign affiliates, you know someone in Lebanon who cheated you. I'm sure that happens sometimes, but the most common perpetrator remains American, typically male, typically age 20-40, often living below his wealth, so living at a standard of living that doesn't reflect the large amount of money he's taking from his victimizing."[9]

MERCHANT FRAUD

The merchants - those paying the commissions - are assumed to be clean, and fair payment of affiliates is required for the entire system to work. However, it has been pointed out affiliates are wary of advertisers who might willfully omit some of the of the sales transactions that should have earned a commission for the affiliate, by deliberately not recording some tracking information or adjusting sales volumes.[10]

Zac Johnson an entrepreneur who has helped affiliates generate millions of dollars, says that an absence of fraud is vital for affiliate marketing to function for those whose career depends on it. "We assume that when we place an affiliate link on our blogs that we will be suitably and accurately credited for any qualified referrals that we generate."

[9] Tune blog, Preventing Affiliate Fraud – Interview with Ben Edelman

[10] Exploring Risk and Fraud Scenarios in Affiliate Marketing Technology from Advertiser's Perspective, Amareskara & Mathrani (2015)

METHODS OF AFFILIATE FRAUD

CHEQ

There are several methods of affiliate fraud that contribute to the $1.4 billion economic losses we expect by the end of 2020

1.COOKIE STUFFING

Browser cookies are the fundamental feature that enables tracking. Cookie stuffing is a process in which an affiliate will place many different cookies belonging to different advertisers (third-party cookies), in the visitor's computer. If the visitor subsequently visits any of those advertisers' sites and makes purchases, the affiliate will earn a commission without actually having taken part in leading the visitor to that site. In 2014, Shawn Hogan, the CEO of a successful online marketing company, Digital Point Solutions, was sentenced to five months in federal prison for his role in defrauding eBay of an alleged $28 million in online marketing fees, in an elaborate cookie-stuffing scheme.

2. ATTRIBUTION FRAUD (APP INSTALLS)

In the same vein, but for mobile apps, attribution fraud is a case where fraudsters attempt to steal credit for app installs, not generated by them. This is an attempt to register the last engagement before the app is first launched by the user. Attribution fraud tricks attribution platforms to associate an organic install or one created by another source to the fraudster, thus manipulating the “last-click-attribution” model commonly applied by attribution providers. For instance, in 2018 Google took again against Cheetah Mobile’s File Manager and the Kika Keyboard on the Play Store. It was alleged they were among a rise in install attribution abuse falsely crediting app installs by creating false clicks. The ongoing Uber case is another example of such attribution fraud. Former Uber head of performance marketing, Kevin Frisch says following an investigation, he turned off $100 million out of $150 annual spend on mobile app installations to get new riders.

He says: “We basically saw no change in our number of rider app installs. What we found was that a number of installs we thought had come in through paid channels, suddenly came in through organic. I started gaining reports and I started seeing things that just did not make any sense. There is an app that has 1000 monthly active users and in theory we got 350,000 installs from them. We kept peeling this back, and we found that someone saw an ad and downloaded and opened the app within two seconds, which is just not possible. We discovered what we had was attribution fraud.” Some cases of attribution fraud may involve malware, in which a program “listens” to the user’s activity and is notified once a new app install starts. The malware will then search for campaigns relating to the relevant app, populating the relevant information into a fake click report, registering the last click engagement to win the attribution for an otherwise organic install or one generated by another media partner.

3. TYPO SQUATTING

In this tactic, affiliates register domain names that are misspellings of merchants' domain names. (Moore and Edelman, 2010).

When a user misspells a merchant's domain name in the way that the affliate anticipated, the user will be sent to the affliate's site, which immediately redirects If the user makes a purchase, the affliate will be credited.In one such case, retailer, Land's End proved in court (2006) that its affiliates failed to disclose that they registered as domain names dozens of misspellings of "Land's End". The defendants sent users to the real Land's End site, but only after funneling them through "affiliate" sites so that the defendants could collect commission.

4. LOYALTY SOFTWARE

Here, affliates place "loyalty" software on a user's computer to remind the user about possible rebates, points, or other benefits from purchasing through certain merchants. The loyalty software automatically sends a user through an affliate's link when the user requests a merchant's site directly. Often, loyalty software claims affliate commission even if the user had never registered with the loyalty service and is incapable of claiming or receiving benefits.

5. DECEPTIVE AFFILIATE MARKETING

Sometimes affiliates ads could be bait for a scam, according to investigations by the Federal Trade Commission (FTC). The FTC for instance cracked down on a low-cost trial scam placed by affiliate marketers. Here, a "free" trial offered up by affiliates ended up on a website that offered the product trial for $1.03. "That amount is not much, but it's not free", the FTC stated. They added: "In fact, people who bought the trial for $1.03 ended up being charged almost $200 monthly for a second product they didn't even want". The FTC also continues to crackdown on expensive schemes promising the "secrets" behind affiliate marketing. In March 2020, affiliate marketers behind My Online Business Education (MOBE) settled FTC charges by paying more than $4 million due to an alleged fraudulent business coaching and investment scheme. Consumers paid as much as $60,000 for MOBE "mentoring" . "These so-called 'affiliates' helped MOBE swindle consumers out of millions of dollars by making outlandish and false earnings claims," said Andrew Smith, Director of the FTC's Bureau of Consumer Protection.

In addition, fraudsters use variations on fake clicks and spamming to obtain credit for sales. A particularly nasty development is that of diverting. Diverting is the practice of diverting traffic from an affiliate's site, When buyers are redirected to a fraudsters site, they canstill make a purchase, but the fraudster rather than the original affiliates receives the commission.[11]

[11] See: Affise, Fraud in Performance Marketing, Trends, Statistics, Solutions. For discussion on diverting.

TIMELINE OF AFFILIATE ALLEGATIONS OF FOUL PLAY

2012
Brothers, Andrew Chiu and Allen J. Chiu, found guilty in the US of a scheme to defraud Nordstrom of more than $1.4 million in commissions and rebates

2013
Two of eBay's super-affiliates were caught and convicted of fraud in 2013, after the use of cookie stuffing as they were paid $28 million in affiliate commissions

2016
Criteo dropped a fraud case in which it alleged that competitor Steelhouse counterfeited clicks to trick companies into attributing sales to its rival

2017
Federal Trade Commission charges online marketing operation for deceptive ad practices, driving users to their website via affiliate networks.

2018
Police arrest Alexander Zhukov, an affiliate fraud "mastermind" alleged to have taken more than $7million from merchants

DECEMBER 2018
Google warns app developers of three malicious SDKs being used for attribution fraud

2019
Uber Fraud Case against AdTech companies claiming $70 million was subject to attribution fraud

2020
Affiliate marketers behind My Online Business Education (MOBE) settled FTC charges by paying more than $4 million for deploying a fraudulent business coaching and investment scheme.

INDIRECT COSTS OF AFFILIATE MARKETING FRAUD

CHEQ

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. 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. Some researchers have concluded that crime's most costly factors stem from these less tangible effects.

The risk of affiliate fraud scares many businesses away from the practice altogether and threatens to damage trust in the growing market that can benefit both brands and affiliates. This could jeopardize the revenue model itself. Sufficiently successful attackers could reduce the revenue for legitimate affiliate advertisers so much that the entire business model no longer works, putting both those free sites out of business and further limiting the ways in which free content can be subsidized online.[12]

[12] Journal of Cybersecurity: June 2016: Characterizing Fraud and its ramifications in affiliate marketing networks: Peter Snyder and Chris Kanich