The state of click fraud in SME advertising

CHEQ ClickCease

Introduction

Small and medium-sized enterprises (SMEs) are the engine of the global economy, with 70% of the world's workers employed in business with between one and 250 people[1]. In the US, small firms employ just over half of the private-sector workforce accounting for two-thirds of new jobs over the past decade.

Online advertising is considered essential for most businesses at a time when 94% of consumers research products online before buying, while three out of five people use search engines as their go-to shopping resource[2].

Many small businesses see up to 80% of their business depending on clicks for revenue, through unprecedented opportunities to target customers using digital advertising platforms. Many SMEs have built their entire businesses, and expansion efforts, through relevant ads using paid search campaigns such as Google Ads, alongside paid social advertising including Facebook, Shopify, and Instagram.

[1] OECD, Entrepreneurship at a Glance, 2017
https://www.oecd-ilibrary.org/employment/entrepreneurship-at-a-glance-2017/enterprises-by-size_entrepreneur_aag-2017-5-en

[2] Google, The Small Business Online Marketing Guide

Click fraud: 14% of clicks on SME ads are invalid

Despite the opportunities available to SMEs through digital advertising, the effects of online fraud have a disproportionately large effect on small businesses. In this report we analyze levels of click fraud on online campaigns by SME companies. Companies purchase Pay Per Click (PPC) ads through contracts with online advertising platforms, most notably Google, under which businesses pay a certain amount of money for a particular number of clicks on PPC ads per day.

Click fraud is the act of clicking on a pay per click advert with no intention of buying or using the product or service. It is usually done by competitors in a cut-throat sector, with the objective to divert or negatively impact the advertiser's budget. In this study we reveal that 14% of all clicks on search are click fraud, based on more than 1.8 billion clicks analyzed across campaigns in more than 70 countries. For SMEs, already with tight margins, this can effectively sink their business if not tackled.

Methodology and key findings:

In this study we reveal for the first time the extent of click fraud for SMEs, based on more than 1.8 billion clicks across small and medium sized online ad accounts, analyzed from May 2019 to May 2020. This encompasses spending by small businesses, across 38 small business sectors advertising in 78 countries.

Further analysis is provided on the most cut-throat sectors for click fraud. These findings are broken down by the world's leading countries for small business online advertising, with special focus on the United States, the UK, and, Australia.

Key findings include

- The average annual rate of global click fraud for SMEs is 14.1% .
- Globally, the top five most affected invalid clicks SME sectors are photography (65% rate of invalid clicks), pest control (62%); locksmiths (53%), plumbing (46%), and waste removal (45%).
- There has been a spike in COVID 19 with a further rise in click fraud peaking at 17% during the crisis
- Countries suffering high click rates include SMEs in France (37%), Australia (18%) the UK (13%) and The United Sates (11%).

The economic costs of click fraud for small business

The average small business using Google Ads spends between $9,000 and $10,000 per month on their Google paid search campaigns, accounting for $100,000 to $120,000 per year. Based on the upper end of advertising on paid search, the average small business can lose more than $15,000 a year to click fraud, usually perpetrated by rivals clicking on ads, or automated fraud, through bots. Like other forms of ad fraud, distressingly this situation has been considered the "cost of doing business".[3]

Draining of money that SMEs can ill afford to lose is bad enough. However invalid clicks perpetrated by competitors also denies small businesses valuable demographic data about prospective customers – with real data on customers supplanted by competitor clicks. This denies companies the opportunity to use data-driven insights gathered on their customers and a chance to ascertain future marketing campaign strategies.

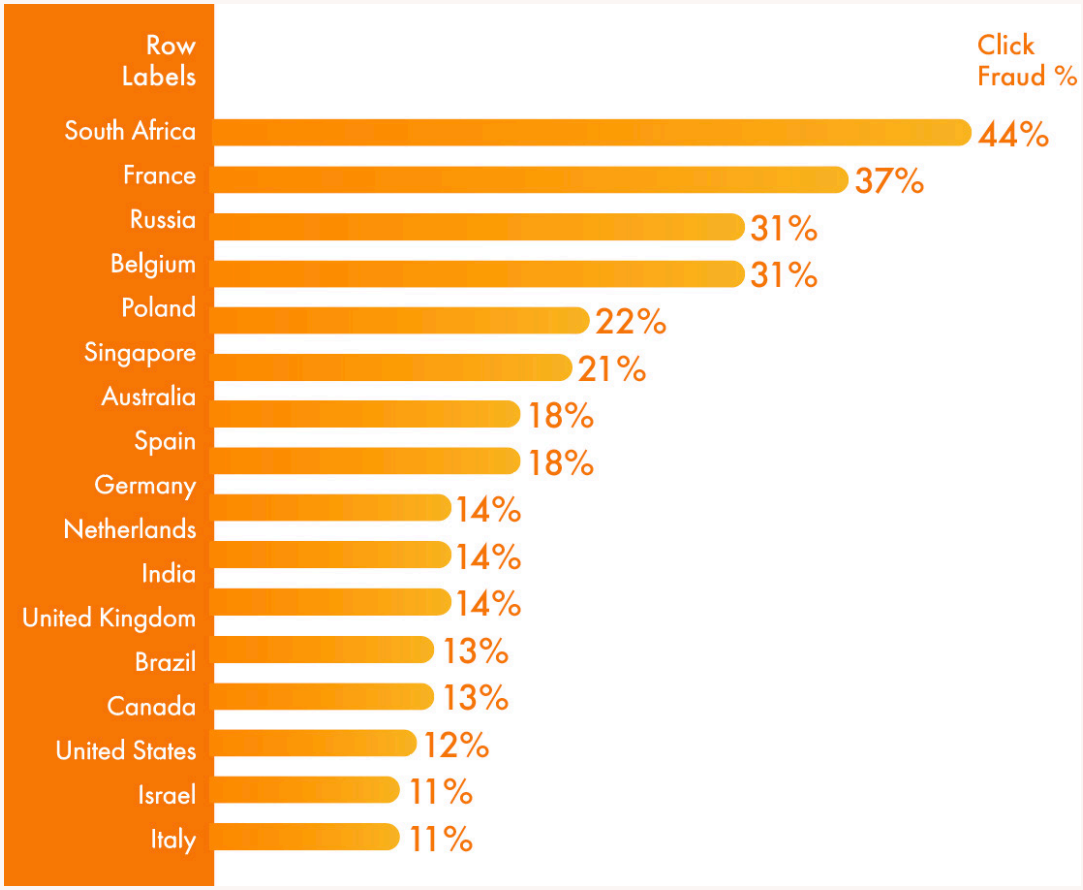
In the words of an ongoing SME court case about competitor click fraud "advertisers are deprived of the value of future customer relationships and acquisition of valuable demographic data regarding viewers who legitimately click on those advertisements."[4]

[3] Nir Kshetri, Professor at University of North Carolina-Greensboro in his book, The Global Cybercrime industry says: "Click frauds are especially painful and frustrating for small companies, which are overwhelmed by search engine marketing budgets and thus are forced to accept fraudulent clicks as a cost of doing business"

[4] Bloomberg Law https://www.bloomberglaw.com/public/desktop/document/MotogolfcomLLCvTopShelfGolfLLCetalDocketNo220cv00674DNevApr102020?1591598036

Click Fraud across the World

Visual representation of click fraud around the world



United States

Number of SMBs:
28.8 million

Click Fraud Rate:
11%

Top 3 US sectors for invalid clicks:

Locksmiths
71%

Pest Control
53%

On-Demand repair
44%

Small businesses in the US are seeing more than one in ten clicks (11%) on their paid search advertising campaigns rendered invalid as a result of deliberate competitor sabotage or bot traffic.

In the US, the most cut-throat click fraud occurred for locksmith ads (71% invalid clicks) which cost around $15 cost per click for the keyword "locksmith". This is followed by pest control (53% invalid clicks) and the on-demand repair sector (44%).

The full challenge for US SMEs is apparent given US SME's reliance on digital advertising. Some 87% of US SMEs advertise online with a primary objective to create sales and revenue (cited as the primary motivation by 32% of US small businesses). The damage has only become more severe with click fraud rates in the US rising to 14% during the peak of the country's COVID outbreak. This is particularly troubling at a time in which 7.5 million US small businesses will shut permanently due distress caused by Covid-19.

Case Study: Las Vegas Golfing company tees off in fight over click fraud

The impact of click fraud on SMEs is highlighted in the ongoing case of Las-Vegas based online golf equipment retailer Motogolf.com. The sports retailer sued a competitor, alleging their competitor violated federal and state law by repeatedly clicking on Motogolf's pay-per-click online Google ads.

According to the court complaint, once viewers have clicked the set number of ads in a given day, the ads become "exhausted" and are no longer visible for potential customers. Beyond having their ads appear on users' web browsers, Motogolf also receives valuable demographic data about prospective customers whenever viewers interact with the online pay-per-click ads. The problem cost the company at least $5000, according to Motogolf. The golf retailer alleged in its complaint that its competitor employees used various electronic devices to intentionally click on Motogolf's online pay-per-click ads "in an illegitimate manner calculated to cause damage to Motogolf".

[5] https://themanifest.com/advertising/small-business-advertising-spending-2019
[6] Ibid

United Kingdom

Number of SMBs:
5.9 million

Click Fraud Rate:
13%

Top 3 US sectors for invalid clicks:
Insurance
37%

Locksmith
26%

Plumbing
16%

In the UK, 13% of clicks on small business online ads are invalid. This is highly problematic given that nearly 80% of SMEs are doing all their marketing online.

In fact, 71% of UK business owners say that online marketing is essential to the success of their business, and in the UK 28% of SMEs said online marketing contributed between 30% and 50% of their annual income. It is in this context that the full impact of click fraud on SMEs is apparent.

Case Study: UK plumbing company finds blockage caused by competitors

Matt Robinson of 12-person Palace Plumbers in the UK says: "Our industry is extremely competitive and I'm sure there are other companies and sole traders that have resorted to sabotaging our account. We rely heavily on online advertising, with 80% of our business currently comes through online ads. This is slowly decreasing as word-of-mouth recommendations and repeat-business increases."

The company spends £3,000 per month on PPC campaigns and believes that losses from click fraud have amounted to "at least a couple of thousand pounds". Robinson adds: "I began to notice that our activity would spike at certain times of the day and deplete our daily budget. This always seemed to be around the daily peak period of 10:00 am -12:00 pm.

Australia

Number of SMBs:
2.1 million

Click Fraud Rate:
18%

Top 3 US sectors for invalid clicks:

Electricians
61%

Pest Control
35%

Plumbing
34%

In Australia nearly one in five clicks (18%) on SME paid search campaigns are invalid, with ads from electricians, pest control, and plumbers facing the highest rates of competitor sabotage. Despite its already high click fraud rate on SME ads, during the peak of COVID 19, click fraud rates in Australia jumped to 28%.

The impact of rising click fraud during the pandemic comes as 63 per cent of Australian small businesses report they have been impacted by the virus, forced to reduce or stand down staff.

Case study: dirty dealings in Waste Disposal

In the field of waste disposal, a specialist in Australia noticed he was receiving outsized clicks on his Google Ads PPC campaigns. This exhausted their budget without a corresponding rise in the number of calls to his business. Using leading click fraud provider, ClickCease, he noticed that the same device IDs were showing up regularly.

The waste disposal manager called around his competitors to ask if they were experiencing similar problems. They were. This led to a planned summit of the six leading waste disposal companies in the city. They all decided to collectively look at their data.

On the day of the meeting, only five of the six competitors arrived. These five competitors discovered they had suffered from the racking up clicks on their ad campaigns– all from the same device ID in the same location in Australia. Everyone agreed it had to be the (no show) sixth player that was clicking on rival ads.

They companies wrote to this suspect and presented their findings. The very next day, the fraudulent clicks stopped, and all of the businesses involved reported that their PPC ads began to behave as expected.

Click Fraud rises by 3% during COVID19

During the COVID 19 pandemic, bad actors online (including competitors) have been pushed to desperate measures, including unfairly competing with rivals through exhausting their PPC campaigns. As Google points out, "hackers frequently look at crises as an opportunity, and COVID-19 is no different".[7] Businesses have suffered from pandemic-related scams, phishing and malware campaigns, and click fraud rates has spiraled as bad actors seek to cut corners and eliminate competitors.

During the rise of COVID 19 from March 2020, click fraud rose from 14%, to a global average of 17%. During March 2020 US SMEs hit 14% for invalid clicks on Google campaigns (from 11% previously), the UK rose from 13 to 21%, and Spain rose from 18% to 23%. In France, with 2.96 million SMEs, click fraud reached a staggering 32%.

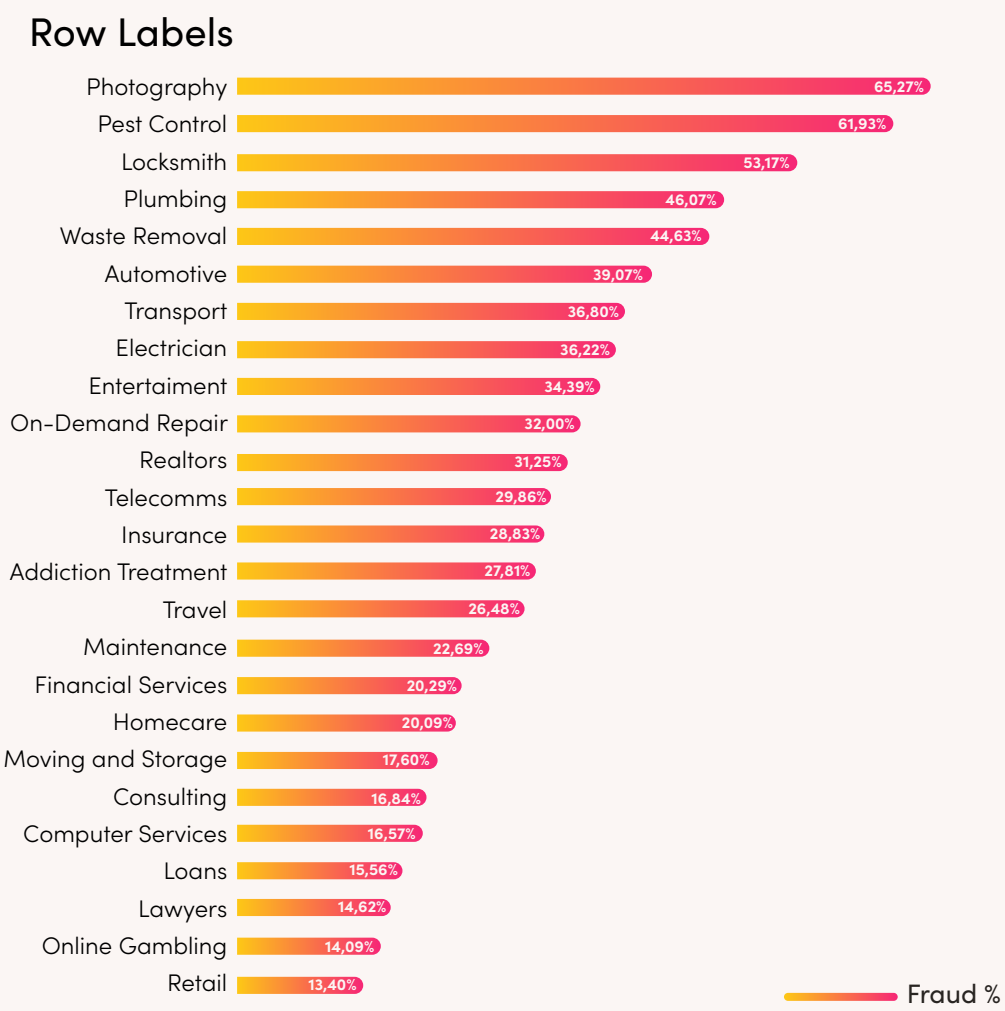
During this period, the highest competitor click fraud was suffered by locksmiths around the world (with a rate of 88% click fraud), plumbers (81%) and realtors (52%).

This online sabotage of SMEs comes as management consultant, McKinsey, estimates that 30 million small-business jobs globally are vulnerable due to the pandemic. Loss of new clients due to wasted advertising spend is a deep problem that SMEs can ill afford at any time, but especially during a global pandemic when job and revenue growth remains extremely depressed.

[7] Google: Findings on COVID-19 and online security threats (April 2020)
https://www.blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats

Sectors most affected by click fraud

Through an analysis of our data we can see click fraud rates by sector. In the following pages we show that there are different characterstics of click fraud depending on the type of SME sector.



[7] Google: Findings on COVID-19 and online security threats (April 2020) https://www.blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats

CHEQ ClickCease

1. On Demand Repair specialists or "Drive-by click fraud"

On Demand Repairs are characterized as professionals, ranging from locksmiths, to plumbers, pest control specialists, to heating and ventilation experts. This group suffers at least a 40% competitor click rate across their PPC campaigns.

The hardest hit are pest control experts who see a 62% rate of invalid clicks; locksmiths, 53%; plumbers, 46%; and waste removal specialists, 45%.

Normally when a consumer needs an on-demand repair service such as a locksmith, they have little need to click an ad multiple times. The usual practice is to find an ad, click on the details and phone to secure a repairer to come to our home. However, repair businesses are seeing their ads clicked 5 to 10 times a day with no accompanying call for services.

Zack Shipman, Senior Consultant at ClickCease says: "We have found it is usually tradesmen driving around in their vans, doing a search for tradesmen in their area and clicking a bunch of times on ads for competitors. In these cases, their daily limit for ad spend is $500 a day, however because of the high cost keywords, at around $50 per click, this budget is exhausted in 10 malicious clicks."

Incentives to click: High-priced SMB keywords (average CPC)

$39 Exterminator	$35.87 Plumber	$14.24 Locksmith	$5.48 Dumpster Rental
$19.93 Electrician	$13.35 Homecare	$15.04 Lawyers Near me	$36 Pest Control

2. Ecommerce and gambling sites: Bot clicks

Online gambling and ecommerce SMEs achieve rates of click fraud at around 14%. Given the lower cost of clicks (usually 10 cents), click fraud usually involves bot traffic clicking on top keywords. Such bots are automated browsers that are programmed by cybercriminals to do a specific set of tasks, like hit webpages to cause ad impressions to load and then click on them. In fact ecommerce click fraud – encompassing attacks against both enterprise and SMEs – is set to cost businesses $3.8 billion in 2020.

3. White-collar click fraud

In the case of landing a real estate listing or a big-ticket client representation, competitors in law firms or rival realtors demonstrate their sharp elbows to sabotage their client's ads. Rates of click fraud among law firms is 15%, however this rose to 17% during May when COVID 19 kept many lawyers in lockdown, and saw even large firms carry out large scale redundancies. Stephan Futeral, CEO of JustLaw, a digital marketing agency for law firms speaking about the considerable impact of click fraud says he managed a PPC campaign for a DUI defense firm spending $20,000 a month. He soon found strange analytics infecting his PPC campaign. He says: "I have encountered substantial fraudulent activities that, if left unchecked, cause significant financial losses and poor campaign performance."

Realtors seeking a high-priced commission engage in click fraud, with invalid rates of 31% on PPC campaigns. This rose to a massive 44% in April 2020 as the impact of COVID 19 brought fierce competition for low numbers of listing opportunities. Homes for sale in the US continue to be in short supply, down nearly 20% compared to a year ago, according to the US Housing Trends report.

4. B2B Click battles

It is not only ads seeking consumer clicks that are sabotaged. Highly competitive B2B software vendors see invalid click rates at 9%. Callum McKeefery Founder & CEO of REVIEWS.io, which offers a solution allowing clients of a business to review their product or service online, says: "This has happened to us a lot. A competitor has continuously clicked on our paid ad. There was one device in Melbourne, Australia that clicked on our ad, once every couple of days, but on really expensive keywords. These keywords cost between $13 and $19 a click. Competitors are doing this on hundreds of devices."

The response of Paid Search platforms

Google, by far the largest player in this market, largely takes a proactive approach to invalid clicks as set out in this report. Any click that is deemed as invalid is automatically filtered from reports and billing schedules – so customers are not charged for them.

If any clicks have escaped their detection filters, customers may be eligible to receive credit for them. However, in many cases clients have found the process is difficult. In the case of on demand repairs, a pattern of five clicks from the same competitor over a period of 30 days may not be seen as necessarily problematic as defined by algorithms (in other sectors customers may click on ad a certain number of times before deciding to purchase).

But in sectors such as plumbers, locksmiths or disposal experts, as we have seen, it is almost certainly click fraud derived from a cut-throat local battleground. London maintenance company, Aspect, which spends up to $130,000 a month on ads found that competitor clicks exhausted their ad spend early in the morning, on a daily basis.

They called for further action to deal with the problem[8]. This has led many to seek out a proactive solution protecting their campaigns across platforms on which PPC ad dollars are spent. The use of click fraud prevention software is growing, including during the COVID 19 recession, where increasing online spend is necessary to promote growth, and protection of this spend is seen as essential.

Small businesses spending on Facebook is another major port of call for businesses seeking growth. In the case of spending on Facebook, new technology has provided larger spending SMEs on the platform with a solution eliminating invalid clicks, protecting their spend.

[8] 28 August 2019: Evening Standard: London Advertiser Aspect calls on Google to tackle "Click Fraud"

Conclusion

The hyper-targeted opportunities available through PPC advertising have become even more important to SMEs, particularly during the COVID 19 crisis. According to Vincent Letang, EVP of global market intelligence at advertising forecaster, Magna, small and local businesses represent 65% to 75% of search and social media spend on Google and Facebook.

Understanding the importance of SMEs both to their future prosperity and the wider global economic recovery, Google has deposited $340 million worth of account credits into SME Google Ads accounts, while Facebook has offered a $100 million grant program, including ad credits to SMEs. In turn, online businesses have taken up the call to advertise and interact online as a necessary measure: with 51% of businesses reporting increased online interactions with their clients.[9]

However, as this new wave of growth arrives, protection of this spending and avoidance of any waste, is fundamental. PPC spending will continue to provide a powerful and proven means for growth for small and medium-sized enterprises. However, as we have seen, the need to tackle the problems of click fraud has become more pressing than ever, at this crucial juncture. Protecting these vital ad budgets from rising click fraud has emerged as table stakes in a wider global mission to create resurgent SME growth into the next decade.

[9] Facebook and Small Business Roundtable: State of Small Business Report