Exploring the Dynamics of Search Advertiser Fraud

Joe DeBlasio[†] Saikat Guha[§] Geoffrey M. Voelker[†] Alex C. Snoeren[†]

UC San Diego[†] Microsoft Research India[§]

{jdeblasio,voelker,snoeren}@cs.ucsd.edu
saikat@microsoft.com

ABSTRACT

Most search engines generate significant revenue through search advertising, wherein advertisements are served alongside traditional search results. These advertisements are attractive to advertisers because ads can be targeted and prominently presented to users at the exact moment that the user is searching for relevant topics.

Deceptive advertising is harmful to all legitimate actors in the search ad ecosystem: Users are less likely to find what they are looking for and may lose trust in ads or the search engine, advertisers lose potential revenue and face unfair competition from advertisers who are not playing by the rules, and the search engine's ecosystem suffers when both users and advertisers are unhappy.

This paper explores search advertiser fraud on Microsoft's Bing search engine platform. We characterize three areas: the scale of search advertiser fraud, the targeting and bidding behavior of fraudulent advertisers, and how fraudulent advertisers impact other advertisers in the ecosystem.

CCS CONCEPTS

• **Information systems** → **Spam detection**; **Sponsored search advertising**; Content match advertising; • **Security and privacy** → *Social engineering attacks*; Economics of security and privacy; *Phishing*; • **Social and professional topics** → *Computer crime*; *Trademarks*;

KEYWORDS

Search advertising, Fraud, Spam, Phishing, Trademark Infringement

ACM Reference Format:
Joe DeBlasio[†] Saikat Guha[§] Geoffrey M. Voelker[†] Alex C. Snoeren[†]. 2017. Exploring the Dynamics of Search Advertiser Fraud. In *Proceedings of IMC '17, London, United Kingdom, November 1–3, 2017,* 14 pages.
https://doi.org/10.1145/3131365.3131393

IMC '17, November 1–3, 2017, London, United Kingdom

ACM ISBN 978-1-4503-5118-8/17/11…$15.00
https://doi.org/10.1145/3131365.3131393

1 INTRODUCTION

Today's Internet ecosystem employs an economic model that delivers free access to a wide variety of services from a host of providers, all underpinned by a common revenue generation mechanism: advertising. Web search engines, in particular, derive much of their revenue from paid search advertisements. Unfortunately, recent reports indicate fraudulent online advertisements are increasingly being used to mislead and even harm unsuspecting Internet users. Savvy web surfers have become rightly wary of clicking on ads, which, in the end, may bite the hand that feeds us all.

By all accounts, online advertising remains a thriving industry. Indeed, Forrester Research reports that online advertising spend will surpass $100 billion by 2019 [26]. Search advertising depends critically, however, on the trust and participation of the public at large. In particular, end users must be willing to click on advertisements that are relevant to them. Hence, fraudulent advertisements have the very real potential to undermine the search ad ecosystem and the services it supports. Such ads display content associated with keywords that users search for and, as with benign ads [30], their goal is to entice users to click on the ad. These fraudulent ads monetize user clicks through a variety of illicit and malicious means, such as selling counterfeit goods, tricking users into paying for online scams like fake anti-virus products, over charging for technical support, or even injecting malware on unsuspecting user's machines.

Given the alarming rate at which new advertising scams seem to appear, it is an open question whether the current model of ad-supported search is sustainable. Very little is publicly known about the vitality of online search advertising as an enterprise, in particular the true costs of fraud and abuse to the search ad networks themselves. Fraudulent ads are a very real problem for search engines, who have strong motivation to defend against them. Although search engines normally profit from users clicking on ads, fraudulent ads often are not billable (if, for instance, the advertiser is using a stolen payment instrument), and, instead, search engines lose legitimate revenue from non-fraudulent advertisements that may be displaced.

We present the first characterization of the fraudulent advertiser ecosystem at Bing, one of the largest search engines, from the perspective of the ad network. Using over two years of data regarding advertiser spend and campaign management, along with user engagement (i.e., impressions, click-through rates, etc.) we measure the scale of the activity, the particular bidding behaviors exhibited by fraudulent advertisers, and the impact those behaviors have on non-fraudulent advertisers.

Our results show that despite a large fraction of new account registrations being fraudulent, Bing successfully prevents most from showing even a single ad. Fraudulent advertisers that do succeed

in posting ads typically survive only a few hours to days and are restricted to a small set of relatively lucrative, but often dubious verticals (e.g., weight loss supplements and designer sunglasses). As such, they have limited impact on non-fraudulent advertisers that tend not to occupy the same verticals. For advertisers who are competing with fraudulent advertisers on dubious verticals, however, increased costs and lower engagement are the norm; verticals engaged by fraudsters are often highly competitive. In sum, we find that Bing's policies, while not perfect, have successfully contained fraud to—for most advertisers, at least—a relatively benign nuisance that may simply be the cost of doing business in today's ad-based Internet ecosystem.

2 BACKGROUND AND RELATED WORK

At a high level, attackers commit fraud in the online advertising ecosystem in two ways. The first is click fraud, in which attackers generate fake 'clicks' to earn payment by posing as the publisher. Click fraud has been extensively studied in the past [4–6, 10, 13, 17, 18, 23, 27]. Efforts have studied both the infrastructure—typically botnets—used to generate the clicks [2, 5, 6, 24] and the quality of the traffic so generated [27, 38]. More sophisticated forms of click fraud are emerging in the mobile space, where unscrupulous actors place ads in locations on the screen where real users are likely to accidentally click on them [16].

In this paper, we focus instead on fraudulent advertisers who post ads to attract legitimate click traffic for a variety of malicious goals, including trying to infect the user's browser with malware (drive-by downloads) [7, 15, 25, 37], stealing email and bank account credentials with fake pages (phishing) [15], collecting personal information to sell to third-party marketing companies (lead generation) [35], bundling malware with software downloads (download stuffing) [11], selling 'miracle' supplements and nutraceuticals (diet or body-building supplements, anti-aging creams, etc.) [14], or perpetrating money-making scams such as convincing the user that their computer is infected with malware and selling them fake anti-virus software [28].

In general, attackers post fraudulent ads at scale in two ways. Either they compromise the accounts of existing legitimate advertisers, or they create new accounts with fraudulent information, including names, email addresses, and credit card information (which is typically stolen). As a result, search engines have stringent account validation (such as credit card verification) for new accounts [8], and also provide tools for advertisers to better protect their accounts [21, 22]. Search engines also proactively attempt to detect fraudulent ads posted by advertisers. When new ads are created, search engines vet the site linked to by the ad at posting, and again when the search engine visits the page over time to update its search index. Search engines have a variety of heuristics to decide whether a page is malicious, such as whether the page delivers content that tries to compromise the browser, scam the user, etc.

Despite these methods, attackers are still able to defeat such approaches, siphoning millions of dollars from search ad networks. Verified accounts are straightforward and cheap to obtain via underground markets [29]. Furthermore, since normal user accounts at Bing, Google, etc. can be converted to advertiser accounts with just additional verification (such as a credit card), as with email and other online accounts, a supply of advertising accounts are inevitably compromised via phishing [12], host or browser compromise [9], etc. Finally, attackers use 'cloaking' on the pages they advertise to evade detection by the search engine crawler. Cloaking has traditionally been used to poison search results [32–34, 36], and attackers have developed many different kinds of cloaking over the years that fraudulent advertisers now also employ. In this paper, it is precisely these fraudulent advertisers that we characterize on the Bing ad network. We seek to understand the scale of fraud, the behavior of fraudsters within the network, and the impact of this fraud on the ad ecosystem.

3 SOURCES AND DEFINITIONS

Our analyses focus on a two-year time span in the recent past, with much of our in-depth analysis focusing on a few representative shorter time periods. We chose this window to be sufficiently far in the past to ensure that most fraudulent actors active during that time have been identified by Bing. Where appropriate, we have verified that more recent data is in line with our analysis. We believe that the trends we report on have not changed significantly during our extended measurement period except where noted.

3.1 Datasets

For the purposes of this paper, we focus on three main data sources:

- **Customer and ad records:** This dataset contains information on each advertiser (when their account was opened, market, language, home currency, etc.), every ad (title, description, display URL and destination URL), keywords bid on, bid types and maximum amounts.
- **Ad impression and click records:** This dataset contains information on ad impressions and ad clicks. In each case, Bing records ad information (advertiser, ad, keywords, etc.), some basic matching information (why the ad matched the query, how much Bing charged the advertiser, etc.), as well as some basic user and query information (search query, market, etc.). This dataset forms the basis for determining how effective a fraudulent advertiser is relative to other advertisers.
- **Fraud detection records:** This dataset represents actions taken by Bing to shut down fraudulent accounts, generated by both Bing's algorithms and manual review. It covers the entire lifetime of the accounts, from creation through long-term monitoring.

3.2 Fraud under measurement

For the purposes of this paper, our designation of 'fraudulent' advertisers are those that Bing has shut down according to their own internal policies [19]. This group primarily includes advertisers who attempt to defraud or deceive either Bing (for instance by providing stolen payment credentials) or Bing's users (e.g., by advertising miracle-cure products or implying that the advertiser is affiliated with a person or organization with whom they are not). Each time an advertiser is shut down by Bing, information about that advertiser's identity and/or advertising campaigns may be blacklisted. Conversely, 'non-fraudulent' advertisers are the set of active advertisers that Bing has not (yet) determined to be non-compliant; it does not include the set of advertisers whose accounts have yet to be granted initial approval.

Bing uses a variety of mechanisms to apprehend fraudulent advertisers, a discussion of which is out of scope of this paper. Many of these mechanisms, however, involve a manual review of the advertiser account in question. This review helps Bing to avoid accidentally shutting down accounts of legitimate paying customers. In addition, in cases where a customer may be out of line with Bing policy, an individual ad or keyword may be removed or otherwise flagged without shutting down the entire account. Thus, accounts that are entirely shutdown are overwhelmingly fraudulent, with the rate of 'friendly fire' being rather low.

There is some amount of inherent subjectivity when it comes to some policies. For instance, Bing's policy forbids claiming a nonexistent affiliation with companies or individuals. But determining when the line has been crossed can be blurry when endorsements are implied rather than stated. On the whole, however, we believe that this definition represents the best ground-truth data available. As with any imperfectly labeled set, our definition may introduce some bias into our analysis. Given that we believe the system minimizes false positives (that is, incorrectly shutting down advertisers), the effects we identify in this work may be slightly under reported.

Our definition also necessarily leaves out other classes of advertisers who are worthy of study. By ignoring accounts that are frozen temporarily, for instance, we may be ignoring a potentially interesting dataset. We performed a manual inspection of advertisers that have been identified by behavioral fraud detection algorithms repeatedly but subsequently allowed to continue advertising to determine if the behavior of these accounts varies from confirmed-fraudulent advertisers. While there are not many of these advertisers, by and large these advertisers were either benign or behave similarly to other fraudulent advertisers, and only manage to evade shutdown by way of narrowly avoiding policy violations. We have found no significant sets of advertisers whose behavior meaningfully differs from other advertisers in their vertical. Further, as policies and algorithms adapt and change, advertisers who previously evaded detection tend to be labeled fraudulent—the observations in Section 5.2 regarding third-party tech support are a good example of this evolution.

We also necessarily omit advertisers who are fraudulent even by current policy standards, but are wholly undetected by Bing's detection methods. While some amount of undetected fraud is inherent in such analyses, we believe that there are several factors that combine to guard against large swaths of undetected fraudulent activity:

- **Bing accepts manual reporting**: Bing accepts complaints from users regarding illegitimate ads. These reports are investigated. If a fraudulent advertiser was not being detected by Bing's internal mechanisms, a user is likely to complain given sufficient activity.
- **Payment fraud detection is high**: For the portion of fraudulent advertisers who use illegitimate payment mechanisms, fraud is often detectable in the form of chargebacks or other indications from the payment network. Moreover, once an advertiser is detected as fraudulent, they may find their payment instruments blacklisted. This restriction effectively forces advertisers defrauding users into also committing payment instrument fraud, as unless the advertiser has access to a large number of genuine payment instruments, payment fraud is necessary to continue operating within the network.
- **We report on activity in the past**: Experience shows that fraudulent advertisers rarely walk away from working accounts. As a result, it is safe to assume that most fraudulent advertisers with meaningful amounts of activity that have not been detected by Bing will remain active until their detection, but also it is likely that Bing will detect this ongoing activity given sufficient time. We take advantage of this by running our analyses on data that is at least 6 months old, and typically much older. By including the oldest data in our analysis, we permit time for Bing to detect as many fraudulent advertisers active in that time period as possible.

Lastly, our data sources also limit insight into fraudulent actors who are unable to successfully open a Bing advertiser account in the first place due to Bing's immediate detection of potential fraud. Given that these actors, by definition, do not show ads and are not visible to users or other advertisers, we consider them to have negligible impact on the ecosystem.

3.3 Subset definitions

To make our analyses more tractable, in many instances we consider subsets of advertisers (both fraudulent and non-fraudulent) to represent the whole. These subsets are each approximately 10,000 advertisers chosen among the pool of advertisers active during the time period.

3.3.1 Fraudulent subsets. We construct four types of fraudulent subsets: a uniformly random selection across all fraudulent advertisers who were alive at any point during the measurement window (labeled 'Fraud'), a uniformly random selection across all fraudulent advertisers whose ads received any clicks during the measurement window ('F with clicks'), and two subsets with weighted probability of inclusion. In the spend-weighted subset ('F spend weight'), fraudulent advertisers are chosen for inclusion with probability proportional to how much money they spend on Bing during the measurement window. The volume subset ('F volume weight') has advertisers chosen with probability proportional to the number of clicks received during the measurement window.

3.3.2 Non-fraudulent subsets. We use a total of seven types of non-fraudulent subsets. Four are defined similarly to their fraudulent counterparts ('Nonfraud', 'NF with clicks', 'NF spend weight', 'NF volume weight')—their selection is designed to represent the non-fraudulent advertisers as a whole, and are used when investigating the effects of fraud on legitimate advertisers. The remaining three subset types are designed to facilitate comparisons between fraudulent and non-fraudulent advertisers of similar ilks and correct for differences in the demographics of fraudulent and non-fraudulent advertisers that would otherwise make behavioral comparison difficult. Each advertiser selected for inclusion is chosen to most closely resemble a corresponding advertiser in the matched subset (that is, chosen to minimize the difference between their corresponding metrics).

'NF spend match' comprises non-fraudulent advertisers chosen to match the fraudulent advertisers in the 'F spend weight' set, where similarity is defined according to amount of money spent. 'NF volume match' corresponds to 'F volume weight' according to click volume. Finally, 'NF rate match' corresponds to a subset wherein non-fraudulent advertisers are chosen to match members

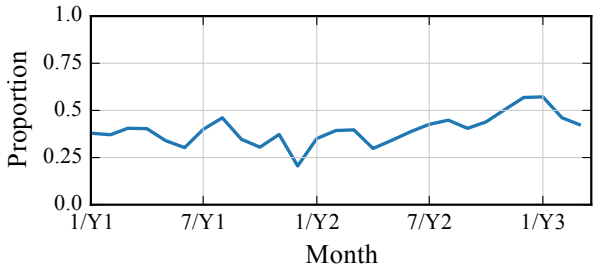


Figure 1: Proportion of active advertisers subsequently marked as fraudulent over time, labeled by end of measurement period.

	#1	#2	#3	#4	#5
all fraud	US	IN	GB	BR	AU
%	50.3	17.2	14.3	2.5	1.8
with clicks	US	IN	GB	BR	CA
%	58.1	14.3	12.3	2.4	1.9
volume weight	US	IN	GB	BR	DE
%	59.5	15.1	8.7	2.6	1.9
spend weight	US	IN	GB	CA	DE
%	60.4	15.1	11.5	1.8	1.7

Table 1: Top-five countries of fraudulent advertisers, as indicated at account registration. We consider four different subsets of fraudulent accounts.

of 'F volume weight' according to the rate at which the advertisers receive clicks during measurement. In both cases, this rate is defined as the number of clicks received during the measurement window divided by the period of time that the advertiser could have been generating activity during that window. That period stretches from the later of the start of the measurement window and the account creation, until the earlier of the measurement window ending or the account being frozen (if applicable).

4 SCALE AND SCOPE

We begin by quantifying the scale of the fraudulent advertising problem at Bing. We start our analysis with account registration, as from the point of view of the search ad network, accounts represent the unit of accountability.

4.1 Account registration

While a single fraudulent actor may register for multiple accounts, an advertiser account is the natural unit of accountability. By this metric, fraudulent advertisers represent a significant challenge for Bing. As shown in Figure 1, during the two years we study, generally more than a third—and near the end more than half—of new account registrations each day are eventually discovered to be fraudulent. The overwhelming majority of fraudulent advertisers have languages, currencies and registered home countries suggesting that fraudsters are based in English-speaking countries—primarily the US and India. Table 1 shows the top-five countries from four different populations

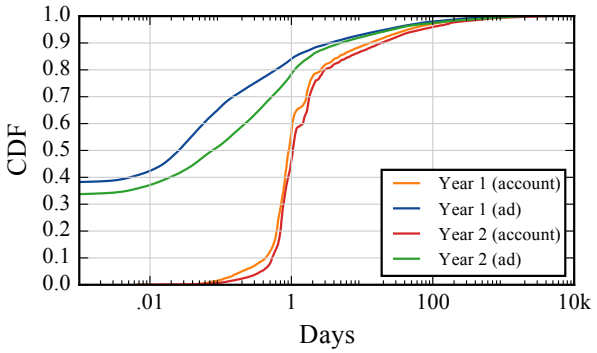


Figure 2: Fraudulent account lifetimes, as measured either from account registration or first ad creation. All fraudulent accounts detected as fraud in first and second year of measurement are shown.

of fraudulent advertisers, each weighted according to the indicated account factor.

Given the high rate of fraudulent account registration, Bing must be vigilant in identifying and acting upon signs of fraudulent activity, which can occur at almost any stage of the account lifetime. 35% of all account shutdowns, however, occur before the advertiser account is able to display even one ad, with the median fraudulent account surviving less than a day from account creation. Of those accounts that are successful in posting any ads at all, most will be shut down within eight hours of beginning to post advertisements, and 90% of all account shutdowns happen within four days of initial ad posting. Figure 2 shows the cumulative density function (CDF) of fraudulent account lifetimes, measured both from account registration and first ad creation. We find that lifetimes are similar in both years of our study.

4.2 Advertiser effectiveness

Despite their relatively short lifespans, fraudulent accounts are able to generate a non-trivial amount of traffic on Bing each month. Over the two-year period of our study, traffic regularly averaged tens of millions of clicks, and over ten million USD losses to Microsoft.

Figure 3 plots the total amount of billable activity or 'spend' and clicks generated each week by the fraudulent accounts present on Bing that week. We break the activity into two categories based upon account. The 'in-window' line includes the activity from accounts detected as fraudulent within a 90-day rolling window starting from the date of activity. The values have been normalize by the maximum value. We observe that fraudulent activity has nearly halved during the period of study.

In contrast, the 'out-of-window' line accounts for activity that was determined to be fraudulent by the end of our study, but not within 90 days of occurrence. We present this line not because it is an accurate accounting of this fraction; indeed, it cannot be: it decreases and necessarily stops approximately 3 months before the end of the figure, as the number of days, and thus opportunities for shut down, approaches zero. Rather, we show it to suggest that our

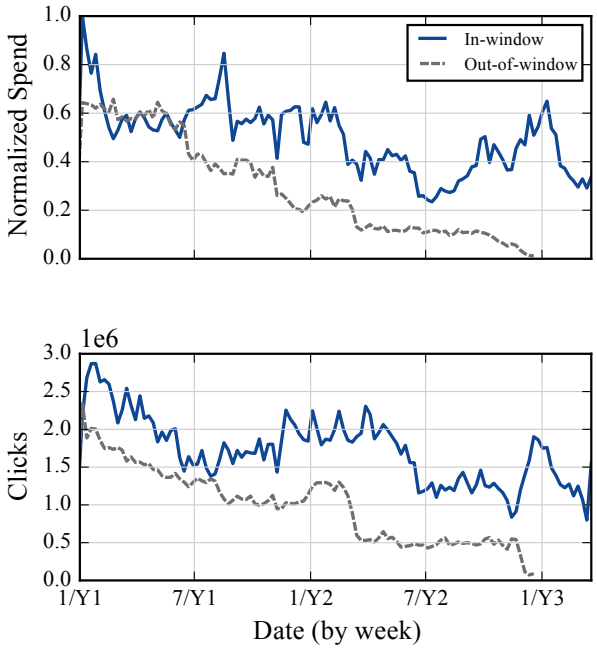


Figure 3: Weekly aggregate fraudulent activity over time. 'In-window' indicates the account detected as fraudulent within 90 days of the given date. 'Out-of-window' indicates accounts that were discovered after more than three months. Spend is normalized by maximum value.

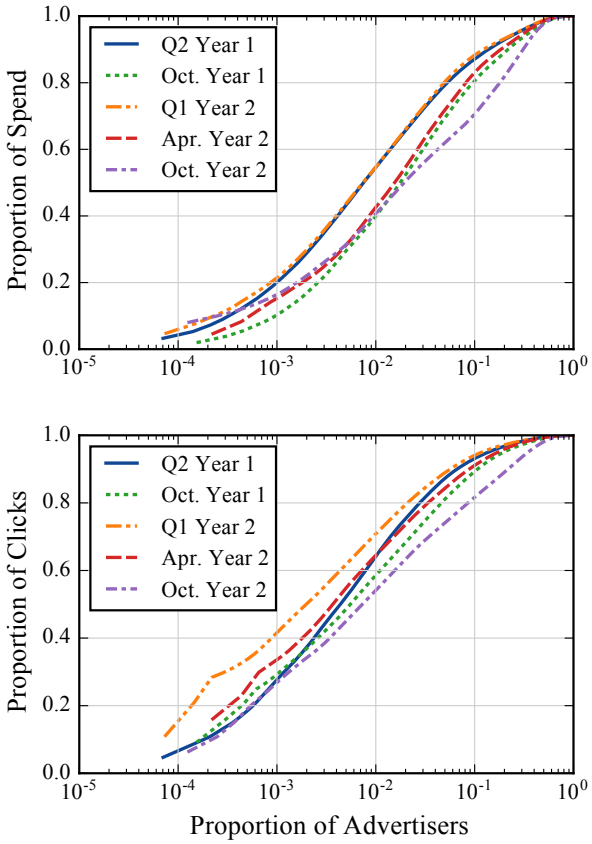


Figure 4: Cumulative proportion of total fraudulent spend/clicks per advertiser for five distinct time periods. Advertisers are in decreasing order of spend.

analyses represent a substantial, but unavoidable, under-reporting of fraudulent activities—potentially by a factor of two or more.

A result of the rapid capture of most fraudulent advertisers is that success is centralized among the top few who dominate the rest. In most time periods, the top 10% of advertisers, as ordered by number of clicks received, collectively account for more than 95% of all fraudulent clicks received. In terms of spend, the situation is similar: the top 10% of advertisers make up 80–90% of spend. Figure 4 shows the distributions of spend and clicks across advertisers over several measurement windows.

Click-through rate (CTRs), the probability that a random user will click an advertiser's ad, provides the primary mechanism for demonstrating ad quality and relevance to search queries. Another metric, cost-per-click (CPC), provides the average amount spent by an advertiser to receive a click. Ad performance, as measured by CTR and CPC, heavily influences whether an ad is shown at all, as well as where the ad appears on the page. While one might expect better performance from fraudulent ads over legitimate advertising, click-through rates for fraudulent advertisers tends to be slightly lower than their non-fraudulent counterparts, only being slightly higher for the highest-spending fraudulent advertisers. Put differently, most fraudulent ads are less alluring to users than legitimate ads, except for the most successful few among them. The fraudulent advertisers that spend the most do so in part because they pay more per click than almost everyone else, existing almost entirely in the upper end of the distribution for cost per click, with CPCs regularly in the several tens of dollars. Many of these advertisers sell products costing more than $100, perhaps permitting such high click costs.

5 ADVERTISER BEHAVIOR

Fraudulent advertisers work hard to attract as many clicks to their ads as possible before they are detected. In doing so, they must be careful when choosing their ads and keywords. Effectively-targeted ads will increase the likelihood that a user will click on the ad, which causes Bing to show the ad more often. Conversely, however, having many ads and keywords that make clear what a fraudulent advertiser is offering provides greater surface area for Bing to detect dubious activity.

5.1 Rates

Figure 5 shows the distribution of impression rates over a representative measurement window. As one might expect, fraudsters show ads more rapidly than their legitimate counterparts. Several reasons contribute to this phenomenon; in addition to fraudsters attempting to gain as much traffic as possible prior to detection, illegitimate

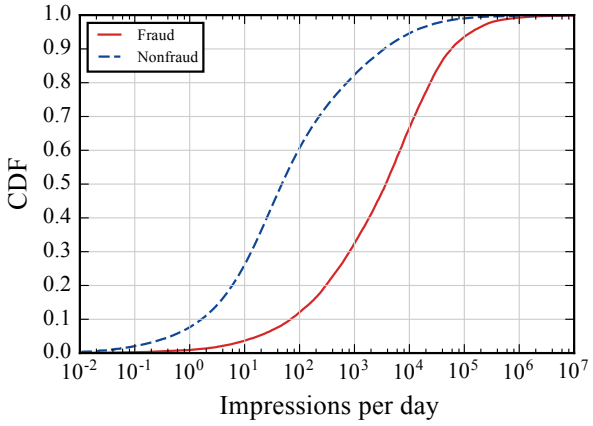


Figure 5: Impression rate witnessed during Year 1 Q2.

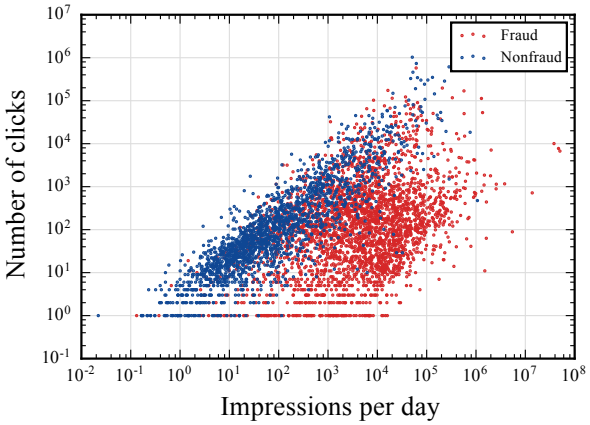


Figure 6: Relationship between impression rate and number of clicks received in Year 1 Q2.

advertisers may have no intention of paying their bill to Bing (e.g. payment instrument fraud), and may operate in affiliate programs that pay out per-click, and are not discerning about their traffic. Click and spend rate distributions (not shown) have similar shifts with respect to non-fraudulent accounts.

The differences in rate between fraudulent and non-fraudulent disappear when one focuses on prolific advertisers, however. Figure 6 shows the number of clicks received as a function of impression rate during the Year 1 Q2 measurement window. The important observation is that, while there is noticeable separation between fraudulent and non-fraudulent advertisers at lower click volumes, higher valued non-fraudulent advertisers are substantially more likely to have rates roughly equaling the performance of similarly-prolific fraudulent accounts. As a result, while rate checks are effective for detecting many low-volume fraudulent users, the most successful fraudulent users blend in with their non-fraudulent counterparts.

5.2 Targeting

Bing determines how often to show ads in part by the performance of the advertisement when shown [3]. As a result, targeting an ad too broadly results in lower relevance to the search queries, which often hurts performance. We find that successful fraudulent advertisers target their audiences similarly to legitimate advertisers [31] (e.g. advertisers that bid on terms such as 'YouTube', 'videos' or 'news' offer ads for sites designed to look like video or news sites), but with the added challenge of evading blacklisted keywords or ad copy that is likely to trigger filters. Moreover, because adding ads and keywords only increases the ways in which the advertiser can be identified (both for current accounts and in the future), fraudulent advertisers are pressured to keep the number of ads and keywords low to reduce the probability of detection.

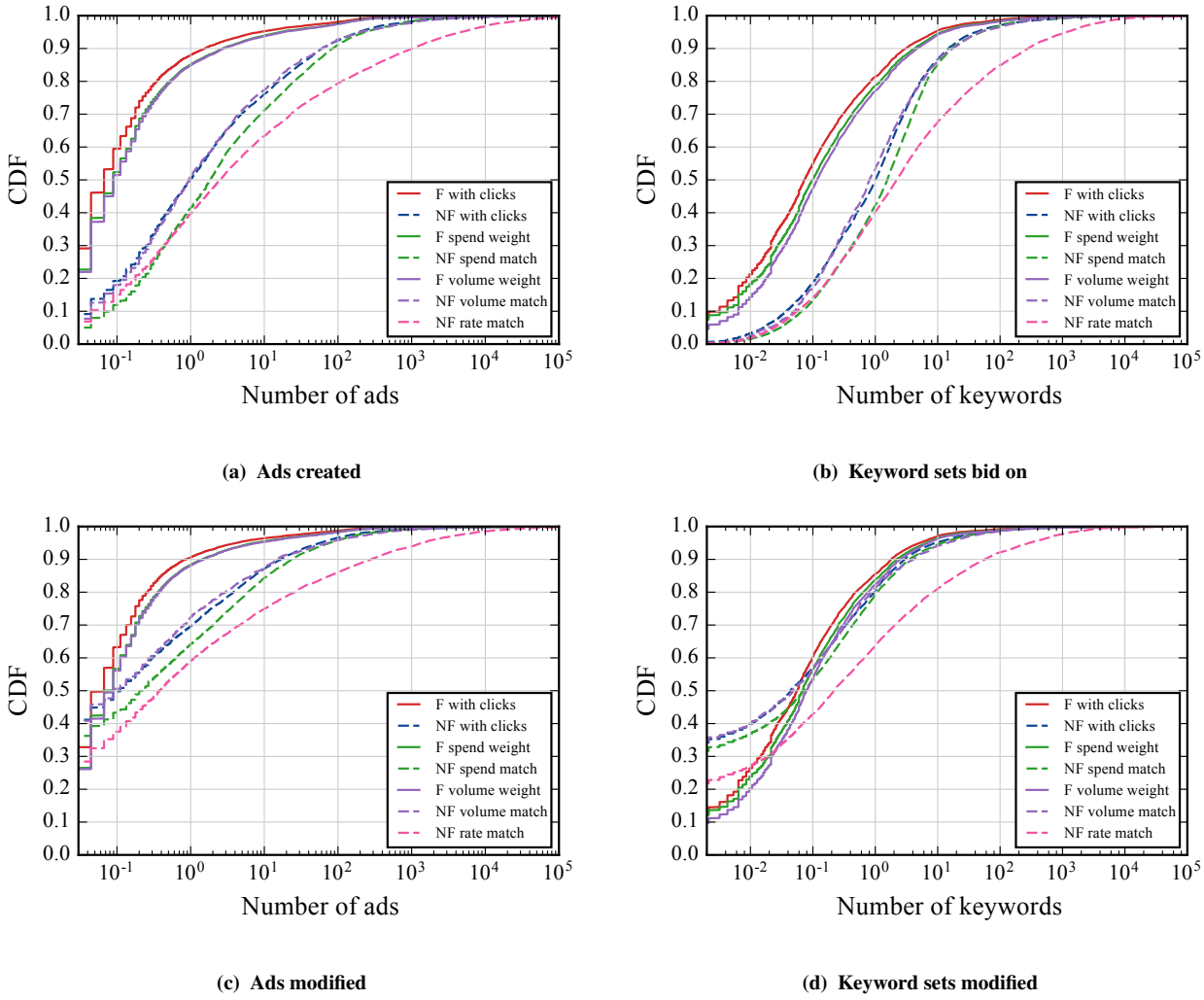
Figure 7 shows the distribution of the number of ads and number of keywords created or modified per account. The total numbers of ads created and keywords on which fraudulent advertisers bid are each more than an order-of-magnitude less than their non-fraudulent counterparts, with the differences greatest when compared to advertisers posting at similar rates to fraudulent advertisers. This is true even though fraudulent advertisers appear to maintain their ads and keyword sets at rates similar to other advertisers. This effect is even more pronounced when compared against non-fraudulent advertisers with similar rates of posting ads, consistent with fraudulent advertisers pushing to receive as much traffic per-ad as possible.

5.2.1 Verticals. Fraudulent ads span a wide array of topics. The significant majority of fraudulent advertisers, however, appear to participate in pay-per-click or pay-per-action affiliate programs. These programs are a popular choice among fraudulent advertisers because they are quick and easy to join and require little sophistication to begin monetizing. Many advertisers involved with the easier-to-join programs advertise for several programs simultaneously, using one advertising account across their campaigns. The highest spending accounts, however, tend to be more focused on fewer, more specialized and lucrative verticals.

The top categories in terms of clicks are typically sites dedicated to offering downloads of popular software. These range from heavily ad-laden sites providing unmodified copies of open source software to sites spreading malware bundled with cracked versions of commercial software. A common strategy is offering open source software bundled with ad-injecting installers.

Figure 8 shows some of the most popular verticals targeted among the most prolific advertisers (in terms of spend) periodically from year 2. Fraudulent advertisers target hundreds of distinct verticals; these verticals were chosen for their prevalence in at least one month. Table 2 provides sample ads for some prominent categories.

The first quarter of the measurement period offers a particularly interesting example of targeted intervention. During that quarter, '`techsupport`' was by far the vertical with the most fraudulent spend. In this model, advertisers offer technical support for business accounting software, printers, routers, antivirus products or other technology, and work by encouraging users to call a phone number, where users pay hundreds of dollars for a single support call.



(a) Ads created **(b) Keyword sets bid on**

(c) Ads modified **(d) Keyword sets modified**

Figure 7: The distribution of ads and keyword sets added or modified as a function of advertiser type from Year 1 Q2. Normalized by median number of creations from 'NF with clicks'.

Category	Ad Title	Ad Body
techsupport	Install Printer	Call Our Helpline Number. Online Printer Support By Experts.
downloads	Discord Free Download	Latest 2017 Version. 100% Free! Instantly Download Discord Now!
luxury	75% Off C0ACH Factory Outlet	Enjoy 75% Off & High Quality C0ACH Bags & Purses. Winter Sale Limited Time Offer
wrinkles	Best Anti Wrinkle Cream	Premium Skin Care Product! Removes Wrinkles in Weeks! Clinically Proven
impersonation	Target - Online Shopping	Store Hours & Locations. Go To Target.com Online Shopping Now.

Table 2: Example ads from selected popular categories.

This vertical was dominated by a few especially prolific advertisers; in the first quarter of year 2, just fourteen advertisers survived long enough to spend more than $100,000, and 134 spent more than $10,000. Of these, 11 of the 14 and 81 of the 134 were selling third-party tech support. In contrast, no other category received more than one advertiser in the top 14, and the second-place holders (a three-way tie) made up just 7 of the top 134.

The precipitous drop-off corresponds to a policy change in which Bing prohibited the marketing of third-party technical support services [1]. Prior to this change, Bing only prohibited advertisers from inaccurately suggesting an affiliation with other companies.

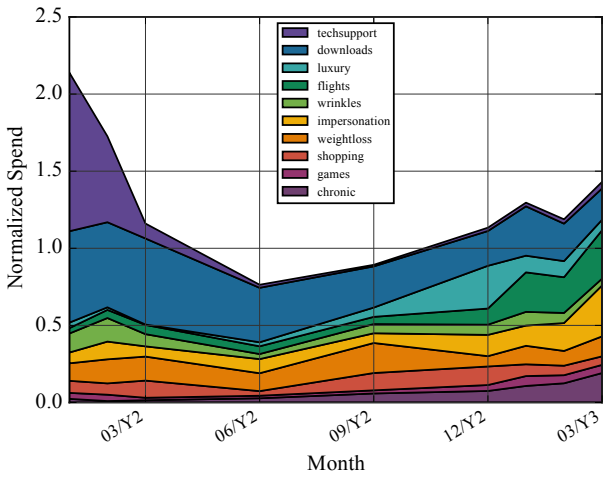


Figure 8: Primary verticals targeted by fraudulent advertisers, manually labeled from ad copy on all advertisers with more than $2000 spend in a month. Amounts are aggregated per-month with data points every three months, with monthly frequency at edges of date range. Data normalized by same value as in Figure 3.

5.2.2 Phishing. One vertical deserves special mention, given its recent prominence in the popular press: phishing. By the numbers, phishing-type scams historically make up only a small percentage of the total fraudulent advertising activity on Bing. When we manually inspected all advertisers in Year 2 Q1 who managed to spend more than $10,000, only one account was used for phishing; most phishing accounts are shut down quickly. Similarly, manual inspection of the most prolific advertisers at various points throughout the measurement period yielded few instances of traditional credential phishing, though there was a noticeable uptick towards the end of our measurement period.

We suspect phishing is somewhat less prevalent than one might expect due to aggressively targeted machine learning and blacklisting. Like all blacklisting, Bing's blacklisting is most effective for high-value targets (like banks) with unique names, as the fraudster must name the institution in order to impersonate it. The blacklisting is less effective, however, in a few cases: when legitimate advertisers may purchase ads targeting the site (e.g. an ad may point to a user's YouTube channel), when the bare company name aliases with a term that isn't easy to blacklist, and where the institution is too small to have yet been added to the blacklist.

Indeed, much of the phishing we observe during the period of study targets small financial institutions and services in non-English-speaking markets where the blacklist is not as developed, and against services whose names cannot be effectively blacklisted. Fraudsters targeting these small institutions can be effective in evading detection for a time, but as blacklists grow, the fraudsters may run out of sufficiently-attractive targets. Impersonation of non-blacklistable companies does pose an ongoing problem.

Country	% of Fraud	% of Country
US	61%	< 2%
BR	10%	< 6%
DE	10%	< 3%
CA	5%	< 2%
GB	3%	< 1%
FR	3%	< 1%
IN	2%	< 2%
MX	2%	< 1%
AU	1%	< 2%
SE	1%	< 2%

Table 3: Country distribution of fraudulent clicks from a typical sample day. '% of Country' indicates the portion of clicks in that country that are to fraudulent accounts.

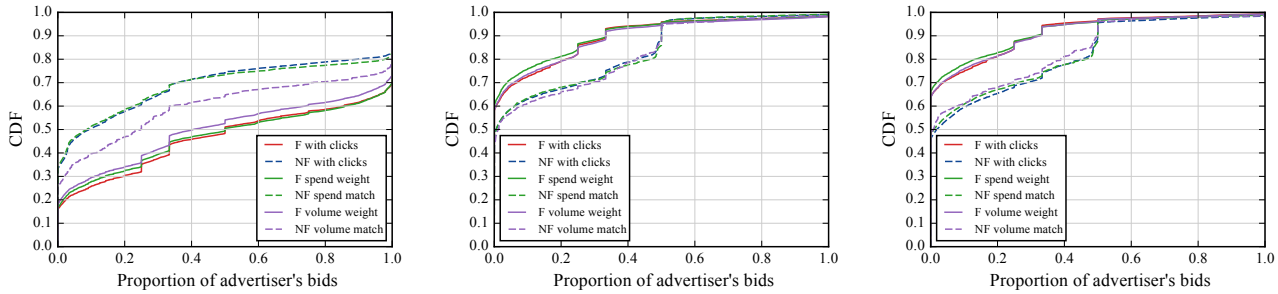
A superset of phishing that we see commonly is impersonation. Impersonation encompasses any time a site attempts to mimic a larger site to attract clicks. Many sites in this category are not attempting to get a user to reveal private information, but are attempting to piggyback on the reputation of the more prominent sites. Streaming sites, rival search engines, large retail establishments, and social networks are all popular impersonation targets. Visitors to these sites may be greeted by any number of scams and low quality advertising.

5.2.3 Geography. Table 3 shows the countries receiving the most fraudulent clicks. The US is by far the most attractive target, but the country with the greatest proportion of fraudulent traffic is Brazil. Interestingly, the UK and France are significantly cleaner overall than other major Western nations. An equivalent breakdown by language yields a very similar result. These results mirror the fraudulent accounts' stated home countries/languages at registration, and by and large, accounts target ads in their own country.

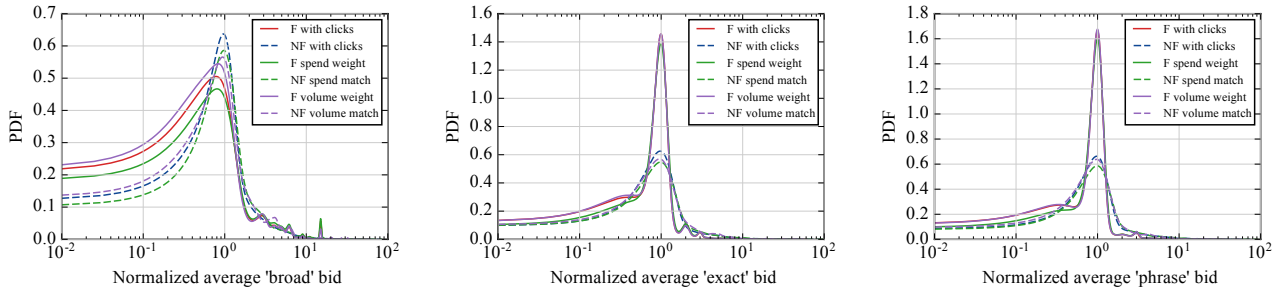
This distribution is likely due to a combination of factors: Bing's differing market share across different markets, local regulation, market forces, relative tuning of detection algorithms and language spoken of analysts, as well as cultural and other factors likely all play a role. We were unable to locate any clear correlations between fraudulent click behavior and country, but we speculate that the size and relative wealth of the markets in each language accounts for much of this distribution.

5.2.4 Blacklist evasion. Bing maintains blacklists of words and patterns (such as phone numbers and some trademarks) that are not permitted in ad text or keywords. By and large, successful fraudulent advertisers rely on phrasing in ads and keywords bid on that are not easily blacklisted outright: e.g., terms like 'news', 'download' or 'skin care' are used by legitimate and illegitimate advertisers alike.

Occasionally, fraudulent advertisers are motivated to circumvent these blacklists, and we see every combination of words using look-alike characters (e.g. 'O' for '0', diacritics). A typical example is the prohibition of phone numbers in ads (since users calling a phone number circumvent Bing's billing mechanisms by not requiring a click). Advertisers often try to avoid detection in these cases by injecting text into parts of phone numbers or presenting numbers in odd formats (e.g. 'CALL 1-800 (USA) 555 1000').



(a) Proportion of offers that are 'broad' offers **(b) Proportion of offers that are 'exact' offers** **(c) Proportion of offers that are 'phrase' offers**



(d) Average 'broad'-match bid per advertiser **(e) Average 'exact'-match bid per advertiser** **(f) Average 'phrase'-match bid per advertiser**

Figure 9: Advertisers' use of Bing's three distinct ad match types in Year 1 Q2. Bid values normalized by Bing's US default maximum bid amount.

Bing also maintains a fairly aggressive blacklist of domains used in fraudulent activities. As a result, the URLs witnessed in fraudulent ads (either as the URL displayed or as the destination URL after a click is received) are typically unique to that account. The most common domains that are shared between fraudulent advertisers are third-party services which also serve non-fraudulent traffic, including URL shortening services (e.g. `bit.ly`) and affiliate programs (e.g. MaxBounty).

The most clicked-on domains are nearly universally unique to individual advertisers (with a few affiliate programs added in). Fraudulent advertisers, however, often use more than one URL. While 74% of fraudulent advertisers use a single domain in their advertisements, and 96% use 3 or fewer, most accounts are shutdown so quickly that these figures are misleading. Predicating on accounts that have multiple ads moves the mean case to 3 domains, with the 90th percentile having nearly 20.

5.3 Bidding style

In Bing's ad platform, advertisers choose a matching method alongside choosing keywords to bid on. During a search, Bing assembles a list of ads that are eligible to be shown using this match method (or 'type') to determine whether the keywords match the search query. Bing supports three distinct types of matches that pair a search query with a given keyword phrase.

An 'exact' match occurs when the keywords chosen by the advertiser occur as the exact search query, with no changes to ordering or additional words. A 'phrase' match occurs when the keywords occur in the right order, but optionally with additional words preceding or following the keywords. Finally, a 'broad' match occurs when the keywords, or any keywords that Bing determines to be similar, occur in the query, regardless of order or existence of other words in the query [20]. Across all match types, Bing normalizes for misspellings, plurals, acronyms and other minor grammatical variations.

For many fraudulent advertisers, the strongest incentive is to ensure that their ad is seen as many times as possible before their deception is uncovered by the advertising network—precise targeting is less important, so long as users still engage. As such, fraudulent advertisers skew away from precision matching, preferring broader matches. While a quarter of legitimate advertisers use exact matches at least a third of the time, only about 10% of fraudulent actors use exact matches that frequently. 60% of fraudulent advertisers do not have even a single exact bid (compared to about 50% of legitimate advertisers). Proportions are similar for phrase matching. In contrast, legitimate advertisers use broad matching less than 10% of the time, while the median fraudulent advertiser uses phrase matching in half of cases. See Figures 9(a), 9(b), and 9(c) for the full distributions.

Table 4 shows the distribution of clicks received according to the matching method employed by fraudulent advertisers. As expected from their targeting strategies, the proportion of clicks from exact matches is lower than in the non-fraudulent population. Interestingly, however, phrase matching is considerably over-represented compared to the non-fraudulent population.

Type	% of Fraud	% of Type	Non-fraudulent %
Exact	61.62%	0.90%	67.88%
Phrase	31.05%	1.32%	23.32%
Broad	7.33%	0.83%	8.80%

Table 4: Match type distribution of clicks received on fraudulent ads on a typical sample day, as compared to non-fraudulent advertisers.

Advertisers may also specify a different maximum bid for each match type and keyword combination. Contrary to our initial expectations, bidding prices among fraudulent advertisers are not significantly different than non-fraudulent advertisers (with the exception of some quickly-caught advertisers). Across all bid types, for both fraudulent and non-fraudulent advertisers, the median maximum bid is the same as the default amount in US markets. The most notable trend in bid pricing for fraudulent advertisers is that only 17% of such advertisers are bidding more than the default on both exact- and phrase-type matches, while non-fraudulent advertisers are roughly double that. See Figures 9(d), 9(e), and 9(f) for the full distributions.

6 THE IMPACT OF FRAUD

The final question we explore is the extent to which fraudulent advertisers impact other advertisers competing in ad auctions. One might expect that because fraudulent advertisers are often not spending their own money, they would be more profligate in their bids. As a result, competing advertisers may lose auctions more often, or potentially have to pay more for ads.

We consider advertisers to be competing with fraud when their ads are shown alongside ads from fraudulent advertisers. We ignore ads that compete in the auction, but are not shown. We believe this to be a safe simplifying assumption as many ads that participate in auction are still shown to the user (at a lower ranking), and in many cases, no ad is shown. Further, the impact of losing bidders is limited to the prices offered by the ads shown at the lowest ad positions.

In most markets, well less than 2% of search queries result in a fraudulent ad being shown, but the effects are not uniformly distributed. Most verticals have no overlap with fraudulent advertising at all, so advertisers within these verticals are essentially unaffected by fraudulent advertisers. For most advertisers, then, fraudulent advertising has little impact. While there are a few markets with much larger rates of fraud, the percentage of fraud tops out at about one in twenty ads shown (see Table 3).

6.1 Frequency of competition

Figure 10 shows the distributions of the proportion of an advertiser's ad impressions that compete with fraudulent ads. The median legitimate advertiser will have less than 0.6% of their ad impressions shown with a fraudulent ad, and the 95th percentile legitimate advertiser has less than 20% of their ads shown alongside fraudulent ads. Even in samples of advertisers with substantial keyword overlap with the most prolific fraudulent advertisers (not shown), less than 2% of the advertiser's impressions were shown alongside a fraudulent ad in the median case. And when non-fraudulent advertisers do encounter fraudulent competition, they are almost always faced with only a single fraudulent ad.

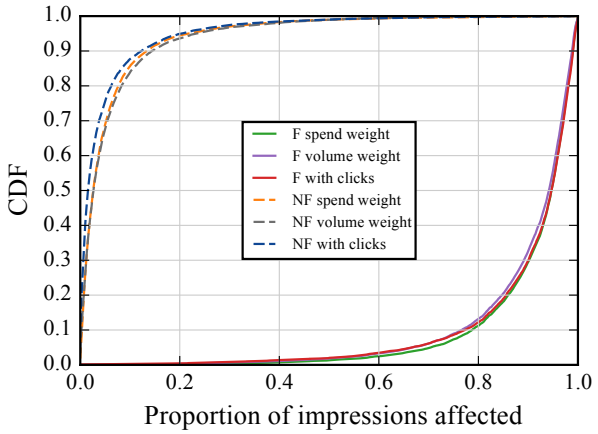


Figure 10: Proportion of impressions affected by fraudulent competition, per advertiser from Year 1 Q2

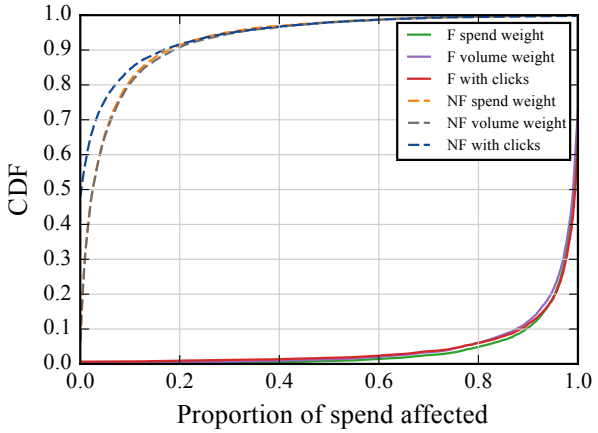


Figure 11: Proportion of revenue affected by fraudulent competition, per advertiser from Year 1 Q2

Fraudulent advertisers often focus on niche areas, and there is substantial competition among advertisers in those verticals. Figure 10 also shows the equivalent distributions for fraudulent advertisers competing with other fraudsters. For the median fraudulent advertiser, more than 90% of their ads will be shown adjacent to a different fraudulent advertiser's ad, and the 95th percentile fraudulent advertiser has nearly all of their impressions in competition with other fraudulent advertisers. Further, in the significant majority of cases, fraudulent advertisers are competing with more than one fraudulent ad shown beside their own (not shown).

The distribution of proportion of spend affected, shown in Figure 11, is similar to the impression distribution with one major difference: a disproportionate amount of the money spent by fraudulent advertisers occurs during heavy competition with other fraudulent

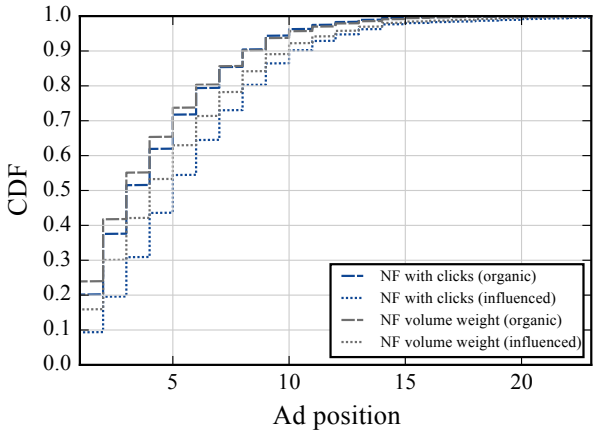


Figure 12: Effects of fraudulent competition on ad position for non-fraudulent advertisers from Year 1 Q2

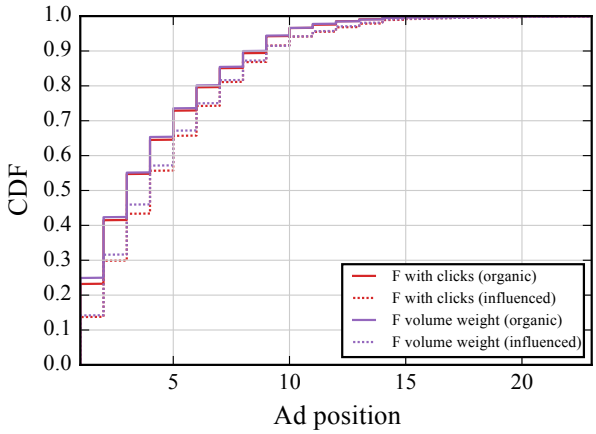


Figure 13: Effects of fraudulent competition on ad position for fraudulent advertisers from Year 1 Q2

advertisers. That is, fraudulent advertisers waste most of their money competing with each other. About 99% of spend is affected by competition from other fraudulent advertisers for the fraudster, compared with just 92% of impressions.

6.2 Impact of competition

While legitimate advertisers do not frequently compete with fraudulent advertisers, when they do, the competition does negatively impact legitimate advertisers—especially when the fraudulent advertisers are operating at volume.

6.2.1 Impact on ad position. On a search engine results page, ads can be displayed along the top of the page (the 'mainline', above traditional search results) or along the right edge of the page ('sidebar'), with the mainline traditionally receiving more clicks than the sidebar, and higher positions in the page typically providing more traffic. In this way, we define 'ad position' as the rank of an ad in the list of ads shown on the page, from the top of the mainline down to the bottom of the sidebar.[1] For ease of comparison, we only examine the effects on ads that were displayed on the first page of results (though fraudulent competing ads may appear on subsequent pages).

Figure 12 shows the impact on ad position of non-fraudulent advertisers competing with fraudulent advertisers for two sets of non-fraudulent advertisers. Other non-fraudulent advertiser subsets show similar effects. Both subsets are from a typical day in our second-quarter Year-1 sample period.

While fraudulent advertisers are only about 5% more likely to achieve the top ad position as compared to their non-fraudulent counterparts absent competition from other fraudulent advertisers, non-fraudulent advertisers are considerably less likely to achieve the top ad position when competing with fraudulent advertisers. The median non-fraudulent advertiser is likely to achieve the top position about 20% of the time without interference (labeled 'organic'); this probability drops to about 10% when competing with fraud (labeled 'influenced'), and similar drops are present throughout the distribution. Put in other terms, competing with a fraudulent advertiser typically costs the legitimate ad about one position. Figure 13 shows the same distributions for fraudulent advertisers, with similar impacts. When fraudulent advertisers compete with each other, however, their probability for reaching the top position drops by about 10%.

6.2.2 Impact on CTR. Competing with fraud has a devastating impact on click through rates (CTRs) among advertisers with lower than median performance. Figure 14 compares the CTRs for non-fraudulent advertisers when competing against other non-fraudulent advertisers ('organic'), and when competing against fraudulent advertisers ('influenced'). While few non-fraudulent advertisers have close-to-zero CTRs when competing on a level playing field, the proportion jumps to 50% when competing with fraud. Even among high-volume non-fraudulent advertisers, CTRs drop by a factor of two in the median case.

A similar, but smaller effect occurs for fraudulent advertisers competing amongst themselves. Figure 16 shows similar CTR distributions for fraudulent advertisers, with and without competition with fraud. Without competition, only a few percent of fraudulent advertisers have near-zero CTRs, but this value jumps to nearly a third with competition. The median case, though, does not experience nearly as significant of a change. Fraudulent advertisers are accustomed to working in a high-fraud-competition environment.

6.2.3 Impact on CPC. While competition with fraud results in a significant increase in the cost per click (CPC) of legitimate ads across the board for the dubious verticals where they compete, this effect is unevenly distributed. Figure 15 compares the CPC distributions for non-fraudulent advertisers with and without competition with fraudulent advertisers, and Figure 17 shows the same CPC

[1] While the '1' slot is always the most valuable position, the number of ads in the mainline and sidebar is dynamic. A particular ad position does not correspond to a particular slot on the page.

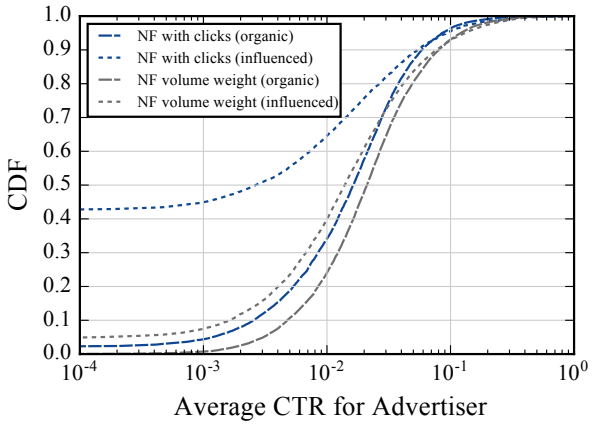


Figure 14: Effects of fraudulent influence on CTR for non-fraudulent advertisers during Year 1 Q2 in dubious verticals

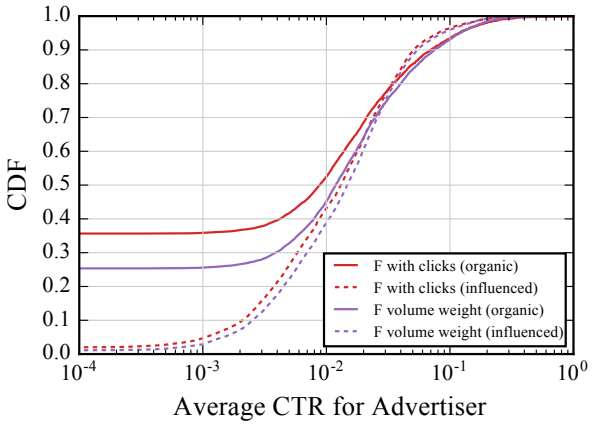


Figure 16: Effects of additional fraudulent influence on CTR for fraudulent advertisers during Year 1 Q2 in dubious verticals

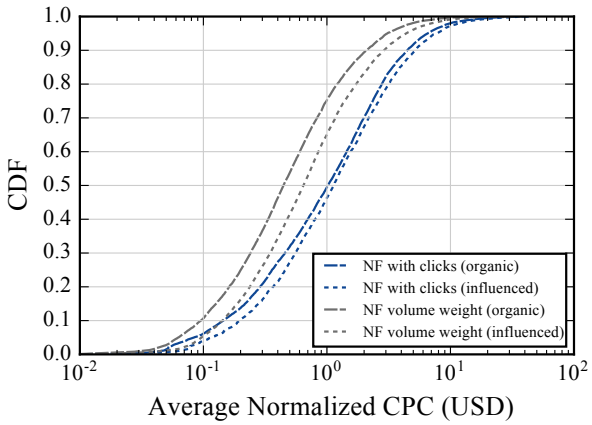


Figure 15: Effects on average CPC per advertiser for non-fraudulent advertisers in dubious verticals. Normalized by median CPC for 'NF with clicks (organic)'

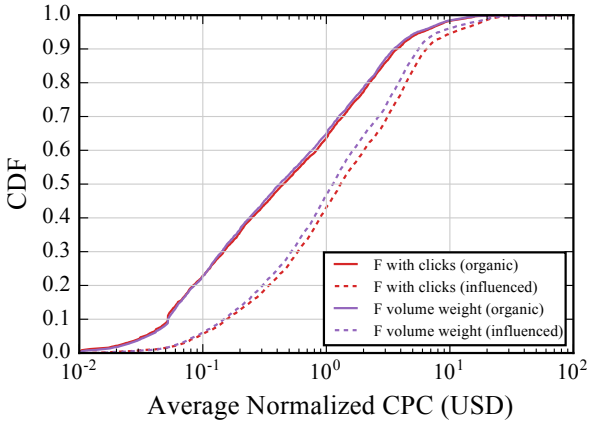


Figure 17: Effects on average CPC per advertiser for fraudulent advertisers in dubious verticals. Normalized by median CPC for 'NF with clicks (organic)'

distributions for fraudulent advertisers. High-volume advertisers in these dubious verticals see increases in CPC around 30% in the median case, while randomly chosen advertisers see impacts less than 5%. Fraudulent advertisers bear an even greater increase. For fraudulent advertisers, CPC increases by around a factor of two when competing with fraud across all subsets of fraudulent advertisers.

7 DISCUSSION

We have explored search advertiser fraud on Bing's search engine platform, quantifying the scale of fraud, the dynamics of being a fraudulent advertiser, and how fraudulent advertisers impact other advertisers in the ecosystem. In this section, we speculate on the implications of our findings for Bing, other search engines, and the advertising ecosystem more broadly.

At a high level, Bing's fraud detection strategies are certainly necessary (e.g. up to a half of new account registrations are fraudulent) and also are effective: fraudulent advertisers who do succeed in evading detection sufficiently long to see non-trivial volume have to operate under considerable constraints and have been relegated to niche aspects of the advertising keyword space. At the same time, fraud is still a significant concern. Fraud costs millions of dollars a month, and fraudulent advertisers are creative and adaptable adversaries constantly probing defenses. So what can Bing, and potentially other mature ad networks, do to further undermine fraudulent advertisers?

Given the mature state of Bing's defenses, new anomaly detection strategies are likely to have diminishing returns. Though many fraudulent advertisers are quickly detected, those that remain are not easily detected by their behavior. Across the variety of features that we examined, effective fraudulent advertisers do not behave substantially differently from legitimate advertisers. For instance, while certain keywords indicate that a market segment might be high risk (and thus perhaps warrant greater scrutiny), it is not the case that successful fraudulent advertisers have keyword or ad copy choices that are sufficiently out of the distribution for non-fraudulent advertisers. In terms of bidding behavior, most of the fraudulent advertisers simply look average with respect to bidding types. Where fraudulent advertisers have higher distributions than their non-fraudulent counterparts (for instance in the proportion of bids that are for a broad match), the spread among fraudulent advertisers is wide enough to be inconclusive.

The ad strategies employed by the prolific fraudulent advertisers are diverse. In some cases, we see advertisers running one or two campaigns at a time, discontinuing old campaigns before starting new ones; in others, we see advertisers constantly adding new ads, allowing the old campaigns to continue uninterrupted. The most prolific fraudulent advertisers even pay their (very large) bills over long periods of time, indicating that it is unlikely that they are using stolen payment instruments. In effect, Bing's defenses over long time periods have coaxed fraudulent advertisers into behaving similarly to legitimate advertisers, precisely to evade anomalous detection.

At this stage of the ad network ecosystem, the most dramatic impacts that Bing (and perhaps other ad networks) can make are by providing targeted policy changes aimed at the most prevalent verticals when they appear, then enforcing checks against that policy. Though we can only speculate on the fraudulent ecosystem experienced in other advertising networks, little of the high-level behavior we have described throughout this paper is likely to be unique to Bing. While any particular bump in a graph may be the result of an action taken by Bing, fraudulent advertisers exploit the gray areas of policy, experimenting with strategies that avoid triggering filters and alarms. If their strategies lead to sufficient issues and complaints, then the ad network can change their policies and broadly undermine fraudulent advertiser activity. Bing's policy change to explicitly prevent advertising of third-party support services had the single most dramatic effect on fraudulent advertiser behavior that we witnessed over two years. Similar such policy changes in the future (e.g. on misleading celebrity branding) are likely to continue to be the most effective instruments of fraud prevention.

ACKNOWLEDGEMENTS

We thank our shepherd Subhabrata Sen and the anonymous reviewers for their valuable feedback. In addition, we are very grateful for the help from Sashank Subhash Kothari, Sarah Ralston, Sean Davis, and Raja Mohan from Microsoft for their willingness to answer questions and point us in the right direction. Finally, we are most indebted to Vacha Dave, also of Microsoft, for time, patience and help in navigating this space. This work was supported in part by National Science Foundation grant 1237264, and by generous research, operational and/or in-kind support via the UCSD Center for Networked Systems (CNS).

REFERENCES

[1] Bing ads policies change log. https://advertise.bingads.microsoft.com/en-us/resources/policies/bing-ads-policies-change-log.

[2] S. A. Alrwais, C. W. Dunn, M. Gupta, A. Gerber, O. Spatscheck, and E. Osterweil. Dissecting ghost clicks: Ad fraud via misdirected human clicks. In *Proc. Annual Computer Security Applications Conf.*, Dec. 2012.

[3] M. Bisson. Bing Ads Auction Explained: How Bid, Cost-per-Click and Quality Score Work Together. https://advertise.bingads.microsoft.com/en-us/blog/post/september-2013/bing-ads-auction-explained-how-bid, -cost-per-click-and-quality-score- work-together.

[4] N. Daswani and M. Stoppelman. The Anatomy of Clickbot.A. In *Proceedings of the First Workshop on Hot Topics in Understanding Botnets*, 2007.

[5] V. Dave, S. Guha, and Y. Zhang. Measuring and Fingerprinting Click-Spam in Ad Networks. In *Proceedings of the ACM SIGCOMM Conference*, Aug. 2012.

[6] V. Dave, S. Guha, and Y. Zhang. ViceROI: Catching Click-Spam in Search Ad Networks. In *Proceedings of the ACM Conference on Computer and Communications Security*, Berlin, Germany, Nov. 2013.

[7] S. Ford, M. Cova, C. Kruegel, and G. Vigna. Analyzing and Detecting Malicious Flash Advertisements. In *Proc. Annual Computer Security Applications Conf.*, Dec. 2009.

[8] Google. Verify your Google Account. https://support.google.com/accounts/answer/63950.

[9] C. Grier, L. Ballard, J. Caballero, N. Chachra, C. J. Dietrich, K. Levchenko, P. Mavrommatis, D. McCoy, A. Nappa, A. Pitsillidis, N. Provos, M. Z. Rafique, M. A. Rajab, C. Rossow, K. Thomas, V. Paxson, S. Savage, and G. M. Voelker. Manufacturing Compromise: The Emergence of Exploit-as-a-Service. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 821–832, Raleigh, NC, Oct. 2012.

[10] H. Haddadi. Fighting Online Click-Fraud Using Bluff Ads. *SIGCOMM Comput. Commun. Rev.*, 40(2):21–25, Apr. 2010.

[11] L. Heddings. Here's What Happens When You Install the Top 10 Download.com Apps. http://www.howtogeek.com/198622/heres-what-happens-when-you-install- the-top-10-download.com-apps/, Jan. 2015.

[12] J. Hong. The State of Phishing Attacks. *Commun. ACM*, 55(1):74–81, Jan. 2012.

[13] A. Juels, S. Stamm, and M. Jakobsson. Combating click fraud via premium clicks. In *Proceedings of 16th USENIX Security Symposium*, 2007.

[14] M. Karami, S. Ghaemi, and D. Mccoy. Folex: An Analysis of an Herbal and Counterfeit Luxury Goods Affiliate Program. In *IEEE eCrime Research Summit*, San Francisco, CA, Sept. 2013.

[15] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang. Knowing your enemy: Understanding and detecting malicious web advertising. In *Proceedings of the ACM Conference on Computer and Communications Security*, Oct. 2012.

[16] B. Liu, S. Nath, R. Govindan, and J. Liu. DECAF: Detecting and characterizing ad fraud in mobile apps. In *Proceedings of the 11th ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, Apr. 2014.

[17] A. Metwally, D. Agrawal, and A. El Abbadi. DETECTIVES: Detecting coalition hit inflation attacks in advertising networks streams. www, pages 241–250, 2007.

[18] A. Metwally, F. Emekçi, D. Agrawal, and A. El Abbadi. SLEUTH: Single-pubLisher attack dEtection Using correlaTion Hunting. *PVLDB*, 1(2):1217–1228, Aug. 2008.

[19] Microsoft. Ad policies and guidelines - bing ads. https://advertise.bingads.microsoft.com/en-us/resources/bing-ads-policies.

[20] Microsoft. Keyword match type options. https://advertise.bingads.microsoft.com/en-us/resources/training/keyword-match-options.

[21] Microsoft. Recent Changes to Improve Account Security in Bing Ads. http://advertise.bingads.microsoft.com/en-us/blog/27853/recent-changes-to-improve-account- security-in-bing-ads, Sept. 2013.

[22] Microsoft. 5 Best Practices When Signing in to Bing Ads with a Microsoft Account. http://advertise.bingads.microsoft.com/en-in/blog/28115/5-best-practices-when-signing-in-to-bing-ads-with- a-microsoft-account, Jan. 2014.

[23] B. Miller, P. Pearce, C. Grier, C. Kreibich, and V. Paxson. What's Clicking What? Techniques and Innovations of Today's Clickbots. DIMVA, pages 164–183, 2011.

[24] P. Pearce, V. Dave, C. Grier, K. Levchenko, S. Guha, D. McCoy, V. Paxson, S. Savage, and G. M. Voelker. Characterizing Large-Scale Click Fraud in ZeroAccess. In *Proceedings of the ACM Conference on Computer and Communications Security*, Scottsdale, Arizona, Nov. 2014.

[25] C. Reis, S. D. Gribble, T. Kohno, and N. C. Weaver. Detecting in-flight page changes with web tripwires. In *Proceedings of the 5th ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, Apr. 2008.

[26] F. Research. US Digital Marketing Forecast, 2014 To 2019. https://www.forrester.com/report/US+Digital+Marketing+Forecast+2014+To+2019/-/E-RES116965.

[27] K. Springborn and P. Barford. Impression fraud in on-line advertising via pay-per-view networks. In *Proceedings of the USENIX Security Symposium*, Aug. 2013.

[28] B. Stone-Gross, R. Stevens, A. Zarras, R. Kemmerer, C. Kruegel, and G. Vigna. Understanding fraudulent activities in online ad exchanges. In *Proc. Internet*

Measurement Conf., Nov. 2011.

[29] K. Thomas, D. McCoy, C. Grier, A. Kolcz, and V. Paxson. Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. In *Proceedings of USENIX Security Symposium*, Aug. 2013.

[30] B. Vattikonda, V. Dave, S. Guha, and A. C. Snoeren. Empirical Analysis of Search Advertising Strategies. In *Proceedings of the ACM Internet Measurement Conference*, Tokyo, Japan, Oct. 2015.

[31] B. C. Vattikonda, S. Kodipaka, H. Zhou, V. Dave, S. Guha, and A. C. Snoeren. Interpreting Advertiser Intent in Sponsored Search. In *Proceedings of the ACM SIGKDD Conference*, Aug. 2015.

[32] D. Wang, M. Der, M. Karami, L. Saul, D. McCoy, S. Savage, and G. M. Voelker. Search + seizure: The effectiveness of interventions on seo campaigns. In *Proceedings of the ACM Internet Measurement Conference*, Vancouver, BC, Canada, Nov. 2014.

[33] D. Wang, S. Savage, and G. M. Voelker. Cloak and Dagger: Dynamics of Web Search Cloaking. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 477–490, Chicago, IL, Oct. 2011.

[34] Y.-M. Wang and M. Ma. Detecting Stealth Web Pages That Use Click-Through Cloaking. Technical Report MSR-TR-2006-178, Microsoft Research, December 2006.

[35] Squeeze page. https://en.wikipedia.org/wiki/Squeeze_page.

[36] B. Wu and B. D. Davison. Detecting Semantic Cloaking on the Web. In *Proceedings of the 15th International World Wide Web Conference*, pages 819–828, May 2006.

[37] A. Zarras, A. Kapravelos, G. Stringhini, T. Holz, C. Kruegel, and G. Vigna. The dark alleys of Madison Avenue: Understanding malicious advertisements. In *Proceedings of the ACM Internet Measurement Conference*, Nov. 2014.

[38] Q. Zhang, T. Ristenpart, S. Savage, and G. M. Voelker. Got Traffic? An Evaluation of Click Traffic Providers. In *Proceedings of the WICOM/AIRWeb Workshop on Web Quality (WebQuality)*, pages 19–26, Hyderabad, India, Mar. 2011.