International Journal of Research in Marketing 41 (2024) 265–281

Contents lists available at ScienceDirect

International Journal of Research in Marketing

journal homepage: www.elsevier.com/locate/ijresmar

Mobile ad fraud: Empirical patterns in publisher and advertising campaign data

Yitian (Sky) Liang [a,*], Xinlei (Jack) Chen [b], Yuxin Chen [c], Ping Xiao [d], Jinglong Zhang [a]

[a] School of Economics and Management, Tsinghua University, China
[b] Cheung Kong Graduate School of Business, China
[c] New York University Shanghai, China
[d] Melbourne Business School, University of Melbourne, Australia

ARTICLE INFO

Article history:
First received on 10 January 2022 and was under review for 7½ months
Available online 28 September 2023

Area Editor: Jie Zhang
Accepting Editor: David Schweidel

Keywords:
Ad fraud
Advertising
Media market
Vertical contract

ABSTRACT

Ad fraud has serious consequences for brands. It also contaminates academic research if scholars neglect a significant level of ad fraud in their data. However, only limited theoretical work has addressed this topic, and empirical research is scarce. In this article, we take a first step to document empirical patterns of mobile ad fraud using two datasets. The datasets are commonly available to buyers of advertising services, and the types of ad fraud studied are significant in the advertising market. We identify some app and campaign characteristics correlated with ad fraud, and uncover methods used by fraudsters to conceal the fraud. They often make the ad fraud proportional to the daily traffic but lowering the ratio of ad fraud on high-traffic days. However, when traffic is unstable, they change strategy to use ad fraud to smooth out the traffic. Meanwhile, in advertising campaigns, the fraudsters allocate most part of fraud during the middle of campaign period, an attempt to reduce the risk of being detected. These findings not only help practitioners and academic researchers determine the extent of ad fraud in the data but also provide stylized facts for future research on theoretical modeling of ad fraud.

1. Introduction

With the proliferation of mobile device such as smartphones and tablets, mobile advertising spending reached $223 billion worldwide in 2022, accounting for 60% of the total digital advertising spending, according to Statista (2022). Relatedly, mobile ad fraud, the practice of fraudulently representing ad impressions, clicks, conversions, app installations, or data events to generate revenue at advertisers' expense, is also catching up with mobile advertising (Loechner, 2019). For example, researchers at the University of Baltimore together with Cheq, a company that helps protect against invalid traffic, found that ad fraud cost marketers more than $35 billion in 2020, and the majority of this occurred via mobile devices (Lynch, 2021). A whitepaper published jointly by Juniper Research and the ad fraud detection company TrafficGuard estimated that one in 13 app installations globally was fake in 2018 (BusinessofApps, 2022). However, given the sophistication of mobile fraudsters in avoiding countermeasures, determining the exact level of damage due to mobile ad fraud is challenging.

* Corresponding author.
E-mail addresses: liangyt@sem.tsinghua.edu.cn (Yitian (Sky) Liang), xlchen@ckgsb.edu.cn (Xinlei (Jack) Chen), yc18@nyu.edu (Y. Chen), p.xiao@mbs.edu (P. Xiao), zhangjl21@mails.tsinghua.edu.cn (J. Zhang).

https://doi.org/10.1016/j.ijresmar.2023.09.003
0167-8116/

Not surprisingly, mobile ad fraud has raised serious concerns from brands and ad agencies. According to eMarketer (BusinessofApps, 2022), 52% of brands and 36% of ad agencies reported that fear of fraud was a concern for in-app advertising. In an Integral Ad Science study conducted in 2019 (BusinessofApps, 2022), 69% of ad agencies and 53% of brand professionals viewed fraudulent impressions as a threat to their digital ad budgets.

Despite the anxiety from the industry, the academic community is relatively silent on this topic. Research on ad fraud is rather limited, with several theoretical studies focused on ad fraud in general, not specifically on mobile ad fraud (Chen et al., 2015; Li et al., 2011; Wilbur and Zhu, 2009). Empirical research is non-existent in the marketing and economic area, and only a few studies have been published in the computer science field (Cho et al., 2016; Liu et al., 2014; Zhang et al., 2011). A direct consequence of this limited research is the lack of empirical knowledge on ad fraud, let alone mobile ad fraud. Furthermore, despite the growing number of studies on digital and mobile advertising, the idea that a significant share of exposures, clicks, or app installations could be fraudulent has seldom been openly addressed.

In this article, we take a first step to document the empirical patterns of mobile ad fraud using two unique datasets. One dataset comes from an advertising network that records ad fraud information of apps registered in the network; hereinafter, we refer to this dataset as "publisher data" and the type of ad fraud in this dataset is the click fraud. The other dataset comes from a brand that records ad fraud information in advertising campaigns conducted by various ad agencies for one digital product of the brand; hereinafter, we refer to this dataset as "agent campaign data" and the type of ad fraud in this dataset is the fraudulent app installation/activation. These datasets are rather common in the advertising market and are suitable to investigate mobile ad fraud. First, they represent common types of data buyers of advertising services (brands or ad agents) can obtain in the advertising market. In the market, an advertising service buyer either purchases traffic directly from publishers or subcontracts with ad agents to design and execute advertising campaigns. In the first case, the buyer obtains data similar to our publisher data, while in the second case, the buyer obtains data similar to our agent campaign data. In addition, academic research on the digital/mobile advertising effect also commonly uses these types of data (e.g., publisher data in Jeziorski and Segal 2015, Sahni and Nair 2022, and Rafieian and Yoganarasimhan 2022; agent campaign data in Braun and Moe 2013, Bruce et al. 2017, and Chae et al. 2019). Second, the types of ad fraud in these two datasets are the major ones in the market. According to Juniper Research (BusinessofApps, 2022), click fraud accounts for 27.3% of the total cost of ad fraud, and fraudulent app installation accounts for 42%.

Our study is descriptive in nature. Given the available information in our data, we try to identify some useful patterns in the mobile ad fraud. For example, which publishers or advertising campaigns have more fraudulent traffic than others? In addition, while it is natural that fraudsters would try to conceal the fraud to avoid the detection, are there certain patterns of ad fraud to achieve that?

Our findings shed some light on frausters' behavior. We do find some app or campaign characteristics correlate with the likelihood of ad fraud. But most importantly, we uncover several ways used by the fraudsters to conceal the fraud. In general, they make the fraud propotional to the daily authentic traffic, but lower the ratio of ad fraud on high-traffic days, an attempt to reduce the risk of being detected. However, when the traffic is very unstable, the fraudersters choose a different strategy by using ad fraud to smooth out the traffic, particularly in the advertising campaign. In that case, they commit less fraud on the high-traffic days but more on low-traffic days. Finally, during a campaign, the fraudsters would allocate most part of fraud during the middle of the campaign period, another way to avoid detection.

These findings provide useful insights into mobile ad fraud. They not only help practitioners determine the extent of ad fraud but also help researchers evaluate to what extent and when they should be concerned about ad fraud in their own research. In addition, these stylized facts can assist future research in theoretical modeling of ad fraud.

We organize the rest of the article as follows: We first provide a literature review on three related streams of research (digital advertising effect, mobile advertising, and ad fraud) and then explain the industry background. Next, we describe the data and present our research questions. We then analyze these questions using our data and provide takeaways of the findings. We conclude with our study's limitations and directions for future research.

2. Literature review

2.1. Digital advertising effect

Many studies have focused on improving the targeting effect of online advertising. Braun and Moe (2013) propose improving advertising performance by varying the creative content shown to an individual, conditional on his or her history of ad impressions. Bruce et al. (2017) construct a dynamic model to examine the joint effects of creative format, message content, and targeting on the performance of digital ads over time. To determine the effect of various advertisements, Li and Kannan (2014) propose a measurement model for conversion attribution in a multichannel online marketing environment. Finally, Chae et al. (2019) caution about the wear-in effect of online advertising campaigns, in addition to the wear-out effect.

Beyond the factors directly related to advertising and consumers, researchers have examined factors such as advertising spillover and competition. Rutz and Bucklin (2011) find a significant spillover from generic keywords to branded keywords in paid search through awareness of relevance. Sahni (2016) examines advertising spillover to the advertiser's competitors on a restaurant search website and finds that ads significantly increase sales for non-advertised restaurants. Jeziorski and

Segal (2015) build a dynamic model to examine how competing ads affect click-through rates. They find that more clicks occur without competing ads.

2.2. Mobile advertising

In addition to digital advertising in general, researchers have specifically focused on marketing through mobile device. Most early studies examined mobile promotions such as mobile coupons or SMS (short message service). Fong et al. (2015) show that promoting to consumers near a competitor's location increases returns to promotional discounts while targeting the focal location produces decreasing returns to deep discounts due to profit cannibalization. Luo et al. (2014) demonstrate the interaction between temporal and geographic targeting. Andrews et al. (2016) show that physical crowdedness increases people's responses to mobile promotions. Zubcsek et al. (2017) find a significant, positive relationship among co-located consumers' responses to mobile coupons.

Research in more recent years has focused on mobile advertising. As a starting point, to determine which products are best suited to mobile advertising, Bart et al. (2014) show that mobile display advertising campaigns significantly increase consumers' favorable attitudes and purchase intentions only when the advertised products are utilitarian (vs. hedonic) and require more (vs. less) involvement. Rafieian and Yoganarasimhan (2022) show that an increase in ad variety in a session leads to a higher response to the next ad. To address privacy concerns, Rafieian and Yoganarasimhan (2021) find that targeting on the basis of behavioral information improves the mobile advertising effect and total surplus but can also reduce an ad network's revenue, which suggests that ad networks have economic incentives to preserve users' privacy without external regulation. Given regulatory concerns about native advertising, Sahni and Nair (2022) find that native advertising in mobile search benefits advertisers, and they detect no evidence of deception under typically used formats of disclosure currently appearing in the paid-search marketplace.

2.3. Ad fraud

Only a few theoretical studies in marketing and economics have analyzed the market impact of click fraud. Li et al. (2011) find that competition among publishers is one reason for the practice of click fraud. They further show that a larger publisher (with a higher number of true clicks) is less likely to commit click fraud and that more intense competition (a higher number of publishers) leads to higher click-fraud rates. Wilbur and Zhu (2009) show that click fraud can benefit the search advertising network depending on uncertainty. Chen et al. (2015) analyze both the advertising network and the advertiser's strategic incentive to invest in click-fraud identification technology. They find that when the cost of technology improvement is high (the likely case in reality), neither party will invest. However, if a neutral third party is involved to resolve disagreements (if any), both parties find it optimal to improve their technology regardless of who (ad network or advertiser) pays the third party.

On the empirical side, apart from the literature on click-fraud detection methods, only a few articles are available in the computer science field. Liu et al. (2014) find that whether an app is fraudulent or not is independent of its ratings and number of ratings. In addition, apps are more likely to be fraudulent in two categories: entertainment and productivity/tools.[1] Zhang et al. (2011) find less fraudulent traffic from higher-priced advertising networks. Finally, in their experiment, Cho et al. (2016) show that most ad networks are vulnerable to ad fraud.

3. Industry background

3.1. Mobile advertising market: Contractual relationship and types of data

A mobile advertising market typically consists of five types of players: advertisers, ad agents, ad networks, publishers, and users. Advertisers are the brands that want to show their ads to users. Ad agents are the firms that contract with advertisers to design and execute advertising campaigns by purchasing online traffic on behalf of the advertisers. Well-known ad agents include WPP in London and Omnicom Group in New York. Ad networks are the marketplaces for advertising service buyers (advertisers and ad agents) and sellers (publishers); they facilitate the matching between ads and online traffic by running real-time auctions. Top ad networks include Google and Facebook. Publishers are content generators (e.g., websites, apps) that attract user traffic. Finally, users are individuals who use mobile apps or browsers to surf online. The roles of ad agents and ad networks can sometimes be obscured because ad networks often serve as ad agents as well.

In Fig. 1, we plot the contractual relationship among players on the supply side of the market (advertisers, ad agents, ad networks, and publishers). The line between any two players indicates a contractual relationship existing in the market, with the direction of the arrow being from the buyer to the seller of the advertising service. In general, the market exhibits a vertical structure, with advertisers as the ultimate buyers located at the top and publishers as the ultimate sellers located at the bottom. The contractual relationship in between these two players is fairly complicated, however. Advertisers often contract with ad agents or ad networks, and sometimes they also directly purchase traffic from large publishers through their in-

[1] Liu et al. (2014) use a finer level of app classification than ours, which contains 18 categories.

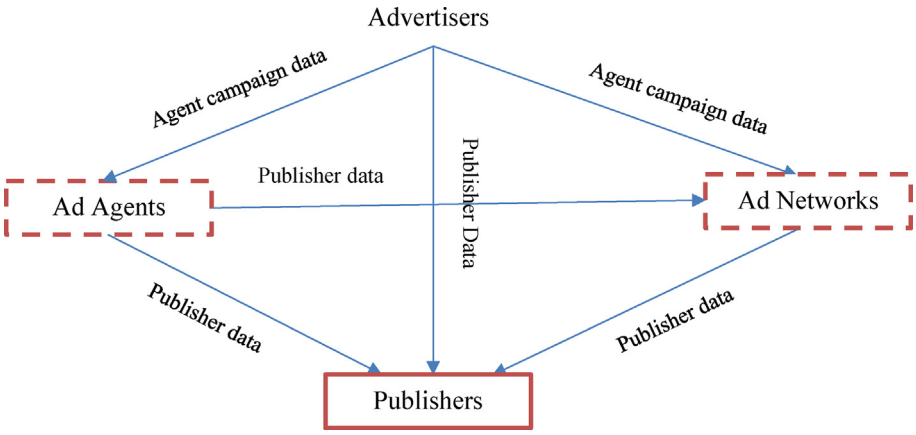

Fig. 1. Mobile advertising market: Contractual relationship and types of data.

house marketing teams. Similarly, ad agents, which design and execute advertising campaigns for advertisers, can purchase online traffic from ad networks or directly from publishers. Finally, ad networks only purchase traffic from publishers.

There are significant variations across contracts and incentives. Publishers are typically paid a piece rate, such as cost per click, cost per impression, or cost per action (e.g., filling out a form, completing a survey, downloading or activating an app). However, the range of the compensation scheme is much wider for ad agents and networks. Many ad agents and ad networks sell traffic in bulk to advertisers at a flat rate. They also guarantee a certain amount of traffic over a certain period (Zhang et al., 2011). In addition, auction-based cost per click and cost per impression are common payment methods for search advertising networks such as Google, Yahoo, and Bing.

In Fig. 1, we also show the types of data an advertising service buyer can obtain from the contract. In general, any contract signed directly with publishers delivers buyers data similar to our publisher data. In addition, ad agents often purchase traffic in bulk from ad networks and obtain publisher data as well. By contrast, the contracts between advertisers and ad agents/ad networks pertain to the design and execution of advertising campaigns, which results in data similar to our agent campaign data.

3.2. Mobile ad fraud: Fraudsters, common tactics, and detection methods

Various players can commit ad fraud in the mobile advertising market. For example, it is well known that publishers can carry out ad fraud. For ad agents, while we found no reliable evidence that they commit ad fraud, we cannot rule out the possibility. Our conversation with industry experts reveals that ad agents may inflat the traffic sometimes to fulfill their contracts with advertisers. The situation is also relatively murky for ad networks. While large ad networks are often trustworthy, some fraudulent ad networks commit or contribute to ad fraud or turn a blind eye to fraud out of conflicts of interest (i.e., while ad fraud drains advertisers' budget, it brings additional revenue to ad networks; Opticks, 2021). Therefore, the ultimate victims of ad fraud are advertisers, which can be taken advantage of by ad agents, ad networks and publishers. Ad agents also suffers from ad fraud, due to ad networks and publishers, which inflates campaign effectiveness in the short run but hurts the agents' reputation in the long run. For ad networks, given their position as intermediaries between traffic buyers (advertisers and ad agents) and sellers (publishers), ad fraud causes little damage to their short-term revenue but hurts their reputation in the long run.

Common types of mobile ad fraud include click spam, click injection, and SDK (software development kit) spoofing. According to Juniper Research (BusinessofApps, 2022), SDK spoofing accounts for 42% of the total cost of ad fraud, followed by click injection (30.33%) and click spam fraud (27.3%).

3.2.1. SDK spoofing

SDK spoofing is a type of bot-based fraud. Fraudsters create artificial installations with data of real devices, which they collect by using their own apps or any apps over which they can gain control (e.g., battery saver, flashlight tool). As the installations appear to be legitimate (fake installations but real devices), SDK spoofing becomes one of the most difficult methods of ad fraud to detect. We thus skip discussion of detection methods for SDK spoofing.

3.2.2. Click injection

Click injection is a sophisticated form of attribution fraud. By publishing an Android app that listens to "install broadcasts," fraudsters can detect when other apps are downloaded on a device and trigger clicks before the installation is fully completed. The fraudsters then receive credit for the installations. One way to detect click injection is to check the click to install time of an installation. An exceedingly low click to install time (<10 s) will be flagged as click injection fraud.

3.2.3. Click spam

Click spam is a form of advertising fraud that involves generating artificial clicks without users' notice. When a user lands on a mobile web page or an app operated by fraudsters, clicks are generated as if the user is interacting with the advertisement, when instead the user is not doing so.

Various methods have been proposed to detect click spam. Some methods identify the fraud by detecting irregular click patterns. For example, analysts can detect duplicate clicks within a short time window from the same device (Zhang & Guan, 2008) or examine suspicious traffic correlation among publishers, given that some publishers do cooperate with each other to commit fraud (Metwally et al., 2007; Stitelman et al., 2013). In addition, Haddadi (2010) proposes the use of bluff ads to detect suspicious publishers and traffic sources (e.g., IP addresses). A bluff ad could either be transparent (invisible to a person) or have irrelevant display text or no content at all (e.g., a blank white picture). As such, users are unlikely to click on the ad. Given this, publishers generating a large number of clicks from bluff ads might attract suspicion, as might the associated traffic sources. Finally, Iqbal et al. (2017) developed a detection method that can be integrated into a desktop or smart device's operating system to check whether a click event is being generated by hardware inputs (e.g., mouse, keyboard, touch) or software-generated simulated events.

4. Data and research questions

As noted previously, we obtain two independent datasets.[2] The publisher data come from an advertising network and contain click-fraud information for mobile apps registered in the network. The agent campaign data come from an advertiser and contain fraudulent app activation information from campaigns the subcontracted ad agent designed and executed. In the following subsections, we describe the data and lay out the research questions.

4.1. Publisher data (click fraud)

We collected the publisher data from a leading mobile advertising network in China (similar to Google's AdMob), which distributes ads to registered apps through an auction-based cost-per-click payment scheme. The payments from the network to the apps are usually on a monthly basis. The data contain an app panel from December 26, 2016, to January 17, 2017. For each app, we observe its daily number of authentic and fraudulent clicks (detected by the advertising network) from all ads. However, we have no information of either the advertisements being clicked or the agents/brands running the ads. The data also contain basic information about the apps, including the app's name and category. We supplement this dataset by collecting additional app characteristics from the leading Chinese mobile application solution company Kuchuan. Specifically, for each app, we collected the number of reviews and review ratings from several major Chinese app stores[3] during the sample period. In addition, for each app, we identify its developer and count the total number of apps developed by this company.

The advertising network employs a specialized in-house fraud detection team. When an app registers with the advertising network, it must integrate with the network's SDK, which is essentially a compiled package of codes. The SDK allows the network to place ads and collect click events in the app. It also allows the network to collect information about the device (e.g., IMEI[4] and sensor data), even though the app is running in the background. The ad network's primary fraud detection method largely relies on such device-level information to determine whether it is a fraudulent device (i.e., a tool specifically used to generate fraudulent clicks, in contrast with a normal user device). If a device is deemed fraudulent, all its clicks are considered fraudulent as well. Although this is a general practice in the industry, we did not have access to the specific input information and detection algorithm; nonetheless, the company provided a simple example. Through the collected sensor information, the advertising network knows the position of the device. If the device stays still for a long time (e.g., several hours), especially during the day, and if this occurs frequently, the algorithm may flag the device as suspicious, because a normal user typically carries a smartphone with him or her during the day.

According to our conversations with industry experts, most apps do not have their own team to commit click fraud; instead, they outsource to third-party companies that specialize in generating fraudulent traffic. For each monthly billing cycle, the ad network notifies each app of its total number of clicks and the number of fraudulent clicks detected. The ad network pays the app only for its authentic clicks.[5] In some cases, if the fraudulent percentage is too high, the ad network will block the app permanently.

4.2. Agent campaign data (fraudulent installation/activation)

The agent campaign data are provided by an advertiser in China that promoted an app with hundreds of campaigns through various agents, some of which are ad networks. These campaigns varied in theme to target different market segments. In the data, campaigns with the same theme could be run by different agents, and an agent can run multiple cam-

[2] Confidentiality agreements prohibit us from revealing the identities of the two data providers.

[3] These app stores include Huawei, OPPO, Tencent's app store, and several other platforms as well.

[4] IMEI stands for International Mobile Equipment Identity, which is essentially the ID of a smartphone.

[5] The app can appeal if it does not agree with the number of fraudulent clicks detected. In such a case, the two parties will engage in a verification process. However, according to industry experts, such cases are rare.

paigns. For each campaign, the advertiser negotiates with the agent for a contract on a cost-per-activation[6] basis. A typical contract includes two components. The first is a minimum number of activations, which the agent guarantees over the campaign period. If this minimum is not met, payment to the agent is reduced. The second is certain thresholds on ad fraud. When a threshold is reached, the advertiser could deduct the payment or even blacklist the agent in the future. The data contain a panel of campaigns from January 1, 2016, to December 31, 2016. For each campaign, we observe which agent ran it, the starting and ending dates of the campaign during the data period, and the total daily number of authentic and fraudulent activations (detected by the advertiser). However, the data do not contain any specific information on contract terms.

As mentioned, the advertiser has its own in-house fraud detection team. To track which campaign an activation comes from, the advertiser dubs a "campaign-ID" into the organic app to create a campaign-specific app. This app is then passed to the corresponding agent and distributed by the agent to downstream publishers (in many cases, via ad networks). For example, the agent can place an ad containing the download link of the app on a publisher's page. Upon clicking the link, an individual will be redirected to the agent's server, and the download of the app begins. After a user downloads, installs, and activates the app, an activation signal with the dubbed campaign-ID is sent to the advertiser's server. At the same time, the app can also collect various device information while running in the background and send the information back to the advertiser's server. Similarly, while we do not have access to the detection algorithm, we suspect that it follows similar logic of the publisher data (i.e., the device information collected by the advertiser's app is its inputs). Upon receiving the campaign-ID, the advertiser only knows which campaign the activation comes from, not the specific publisher. If the activation is fraudulent, it could come from either the publisher or possibly ad networks. However, the advertiser cannot tell the origin. During the campaign contract settlement, the advertiser notifies the responsible agent of the total number of activations and the number of fraudulent activations detected. The advertiser then pays the agent according to the contract.[7]

Before going ahead with our sample construction, we need to mention a caveat with regard to the data. Currently, there is no perfect fraud detection method on the market. Therefore, the ad fraud information in our data is not 100% precise. The only party that has complete information about ad fraud is the fraudster; however, it is difficult, if not impossible, to obtain such information from fraudsters. Sometimes experiments can also be an option, in which the researcher creates ad fraud purely for research purposes (e.g., Cho et al., 2016), but this approach only severs to evaluate the market response to ad fraud, not the ad fraud behavior itself. Despite this caveat, these kinds of data are the best available information so far and used by firms to make business decisions, as they contain valuable, though noisy, information about ad fraud. As new detection algorithms are developed, data quality will improve.

4.3. Research questions

As we stated previously, the purpose of this article is to provide firsthand empirical evidence of ad fraud. What does the available information in the datasets indicate about mobile ad fraud? We think there are two questions that could be addressed using our data.

First, does the likelihood of ad fraud correlate with some observable app or campaign characteristics? This question may be the most intuitive given our data. If such a correlation exists, practitioners and academic researchers could assess the extent of ad fraud in the data. In our case, we can well address this question using the publisher data, given the relative rich information on app characteristics, but less so for the agent campaign data, given the limited agent and contract information.

Second, while it is certain that fraudsters would try to conceal the fraud to avoid detection, can we identify some patterns of that in our data? Conceptually, we speculate that fraudsters' behavior could be correlated with firm- and market-level factors. In addition, a temporal effect could arise in the agent campaigns from the contractual restriction on the campaign length and requirement on the minimum number of activations. By examing the correlations between ad fraud and these factors, we aim to uncover some of fraudsters' patterns to conceal fraud. Specifically, we address two questions.

1) Does ad fraud correlate with the authentic traffic (click or activation)? Authentic traffic may be the most significant market information in this context. The correlation between the fraudulent and authentic traffic reveals whether ad fraud is sporadic or somehow deliberate, which is important for researchers to construct theoretical models of ad fraud. Practically, such a correlation also helps determine the level of ad fraud. For example, if the likeihood of ad fraud increases with the amount of authentic traffic, a campaign with good online traffic may have more doubt about its real efficacy.
2) Does the ad fraud exhibit temporal variations? Although publishers have no clear incentive to commit fraud related to timing, timing is particularly relevant for agents, due to the restriction on minimum activations and the contract length. Facing the pressure to fulfill contract requirements, do agents try to either front-load or back-load ad fraud during a campaign?

[6] An activation means a user downloads, installs, and then launches the advertiser's app.

[7] The agent can appeal if it does not agree with the numbers. In such a case, the two parties will engage in a verification process, but such a case is rare.

We can address all these questions with the available information in our data. Answers to these questions will not only provide firsthand information about the extent of ad fraud in the data but also shed light on the possible mechanisms of ad fraud, which are crucial for a theoretical examination of this topic in the future.

5. Empirical analysis: Publisher data

5.1. Sample for analysis

The publisher data contain a random sample of 908 apps with 15,335 app-day observations from December 26, 2016, to January 17, 2017. Not every app has click observations on each day during the data period. If we calculate the daily percentage of apps with click observations, the first two days in the sample show a much lower number (mean 42%, maximum 58%) than the rest of the data period (mean 76%, minimum 66%) for unknown reasons. Therefore, we drop the first two days of observations in the sample. We then exclude apps with fewer than 10 observations[8] to ensure enough information for each app in the calibration sample. The final sample contains 706 apps and 13,570 observations. The advertising network classifies apps into several categories, including entertainment, game, sports, video/music, reading, finance, tools, news/information, and social. We further consolidate them into three categories: utility (249 apps), entertainment (447 apps), and social (10 apps).[9]

For each app, we calculate several aggregate measurements and report the summary statistics in Table 1. On average, an app has 19 days of observations. During the data period, an app generates 26,000 authentic clicks on average, or approximately 1,260 each day. The variation of daily authentic clicks is large, with an average coefficient of variation (mean/standard deviation) of 3.71. Among different types of apps, utility apps generate the most authentic clicks, approximately 1,460 per day, followed by entertainment (1,170 per day) and social apps (450 per day). We measure the extent of ad fraud by fraud rate, i.e., the ratio of fraudulent clicks to total clicks. For the apps in our data, the average daily fraud rate is 13%, and it is similar across the different types of apps, with utility apps' fraud rates slightly higher. Approximately 62% of the apps have at least one review, and the variation across apps is large. For apps with reviews, the average rating is 3.41, with a standard deviation of 1.14.

5.2. Does the likelihood of click fraud correlate with apps' characteristics?

In this analysis, we treat each app as one observation and examine the correlation between the likelihood of click fraud and some observable app characteristics. For each app, we use its average daily fraud rate as the measure of the likelihood of ad fraud, where the fraud rate is defined as the ratio of fraudulent clicks to total clicks. For the independent variables, in addition to the category information in the data, we focus on three other variables for each app: (1) ability to attract authentic clicks, which we measure by the mean and coefficient of variation of the app's daily authentic clicks during the data period; (2) awareness and popularity in the market, which we measure by an app's number of reviews and the average review rating; and (3) size of the app developer, which we measure by the number of apps developed by the focal app's developer. We run the following regression:

$$\begin{aligned} Fraudrate_i = {} & \alpha + \beta \cdot Category_i + \gamma_1 \cdot log(M\_Authentic_i) + \gamma_2 \cdot CV\_Authentic_i + I(N\_Review_i > 0) \\ & \cdot [\delta_1 + \delta_2 \cdot log(N\_Review_i) + \delta_3 \cdot M\_Rating_i] + \theta \cdot log(N\_App\_Parent_i) + \epsilon_i, \end{aligned} \tag{1}$$

where i denotes the app, $Fraudrate_i$ is the average daily fraud rate for app i during the sample period, $Category_i$ is a set of dummies to indicate which category app i falls into, $M\_Authentic_i$ is the mean of daily authentic clicks for app i during the sample period, $CV\_Authentic_i$ is the coefficient of variation of daily authentic clicks for app i during the sample period, N_Review_i is the number of reviews for app i, and M_rating_i is the average review ratings for app i. As some apps have no reviews, we interact the review and rating variables with an index function $I(N\_Review_i > 0)$, which equals 1 if the number of reviews is greater than zero. Finally, $N\_App\_Parent_i$ is the total number of apps developed by app i's developer.

We present the results in column 1 of Table 2. With regard to the ability to attract authentic traffic, we do not find a significant relationship between the likelihood of fraud and the mean daily authentic clicks. However, the likelihood of fraud is negatively correlated with the coefficient of variation of an app's daily authentic clicks. This implies that the higher degree of uncertainty in attracting authentic traffic could lessen the likelihood of click fraud. None of the effects of user review/rating is significant. This finding is consistent with that of Liu et al. (2014), who show that whether an app commits fraud or not does not depend on its rating or number of ratings. Finally, the size of the portfolio of an app's parent company is not significantly correlated with the tendency to commit fraud.

The results also show that entertainment apps are less likely to commit fraud in general. To further examine whether the correlations between likelihood of ad fraud and app characteristics also vary across app categories, we interact the category dummies with app characteristics in the regression. We report the results in column 2 of Table 2. While there is no

[8] These apps only contribute 2.2% to the total authentic clicks and 4.0% to the total fraudulent clicks.

[9] The mapping is as follows: the original categories of "entertainment," "game," "sports," "video/music," and "reading" fall into the new category "entertainment"; the original categories of "finance," "tools," and "news/information" fall into the new category "utility"; and the original "social" category remains the same as the new category "social.".

Table 1
App-level summary statistics for the publisher data.

Category	*Variable*	*Mean*	*SD*	*Min*	*Max*
All	N. of observations	19.22	3.20	10.00	21.00
(706 apps)	Total authentic clicks (10^4)	2.60	5.83	0.06	47.62
	Mean daily authentic clicks (10^3)	1.26	2.78	0.06	22.68
	Coefficient of variation of daily authentic clicks	3.71	1.81	0.49	15.36
	Mean daily fraudulent rate	0.13	0.10	0.03	0.83
	Corr(daily authentic clicks, daily fraudulent clicks)	0.75	0.24	−0.14	1.00
	N. of reviews	832.98	3834.86	0.00	57471.00
	Dummy(N. of reviews > 0)	0.62	–	–	–
	Mean review rating*	3.41	1.14	0.00	5.00
	Mean N. of apps under the parent company	29.17	72.97	1.00	490.00
Utility	N. of observations	19.62	2.95	10.00	21.00
(249 apps)	Total authentic clicks (10^4)	2.99	5.95	0.11	43.45
	Mean daily authentic clicks (10^3)	1.46	2.85	0.06	20.69
	Coefficient of variation of daily authentic clicks	3.79	2.12	0.49	15.36
	Mean daily fraudulent rate	0.15	0.13	0.03	0.83
	Corr(daily authentic clicks, daily fraudulent clicks)	0.75	0.25	−0.03	1.00
	N. of reviews	1033.34	4102.13	0.00	39392.00
	Dummy(N. of reviews > 0)	0.70	–	–	–
	Mean review rating*	3.38	1.20	0.00	5.00
	Mean N. of apps under the parent company	11.75	33.54	1.00	490.00
Entertainment	N. of observations	19.04	3.29	10.00	21.00
(447 apps)	Total authentic clicks (10^4)	2.42	5.81	0.06	47.62
	Mean daily authentic clicks (10^3)	1.17	2.76	0.06	22.68
	Coefficient of variation of daily authentic clicks	3.67	1.61	0.73	11.33
	Mean daily fraudulent rate	0.12	0.09	0.03	0.74
	Corr(daily authentic clicks, daily fraudulent clicks)	0.75	0.23	−0.14	1.00
	N. of reviews	736.38	3720.90	0.00	57471.00
	Dummy(N. of reviews > 0)	0.57	–	–	–
	Mean review rating*	3.41	1.10	0.00	5.00
	Mean N. of apps under the parent company	39.44	86.62	1.00	449.00
Social	N. of observations	17.50	4.14	12.00	21.00
(10 apps)	Total authentic clicks (10^4)	0.90	0.92	0.14	2.91
	Mean daily authentic clicks (10^3)	0.45	0.42	0.11	1.38
	Coefficient of variation of daily authentic clicks	3.72	1.76	1.59	6.69
	Mean daily fraudulent rate	0.13	0.06	0.07	0.26
	Corr(daily authentic clicks, daily fraudulent clicks)	0.79	0.18	0.47	0.98
	N. of reviews	162.60	338.87	0.00	1084.00
	Dummy(N. of reviews > 0)	0.60	–	–	–
	Mean review rating*	3.97	0.80	2.40	4.69
	Mean N. of apps under the parent company	4.20	4.83	1.00	17.00

Notes: For "Mean review rating," summary statistics are calculated on the basis of apps whose numbers of review are positive. For the other variables, the summary statistics are calculated using all apps.

significant difference in these correlations between utility and social apps, there are differences between utility and enterrainment apps in the correlations between likelihood of ad frand and mean daily authentic clicks, whether there is review, and the average review rating.

5.3. Does click fraud correlate with the number of authentic clicks?

We answer this question in a sequential manner. First, we examine whether the daily amount of fraudulent clicks correlates with that of the authentic clicks. If it does, we examine which observable factors moderate the correlation. Second, we examine whether the daily likelihood of click fraud (i.e., the ratio of daily fraudulent clicks to daily total clicks) correlates with the number of authentic clicks. In other words, does the daily percentage of fraudulent clicks increase or decrease with the daily number of the authentic clicks?

5.3.1. Correlation between numbers of fraudulent and authentic clicks

We regress each app's daily number of fraudulent clicks onto its daily number of authentic clicks, while interacting with the same set of variables as in Eq. (1):

$$\begin{aligned} Fraud_{it} = [&\alpha + \beta \cdot Category_i + \gamma_1 \cdot log(M\_Authentic_i) + \gamma_2 \cdot CV\_Authentic_i + I(N\_Review_{it} > 0) \\ &\cdot (\delta_1 + \delta_2 \cdot log(N\_Review_{it}) + \delta_3 \cdot M\_Rating_{it}) + \theta \cdot log(N\_App\_Parent_i)] \cdot Authentic_{it} + \mu_i + \tau_t + \epsilon_{it}. \end{aligned} \quad (2)$$

where i denotes the app, t denotes the day, $Fraud_{it}$ is the daily number of fraudulent clicks for app i on day t, $Authentic_{it}$ is the daily number of authentic clicks for app i on day t, N_Review_{it} is the number of reviews for app i before day t, M_Rating_{it} is the

Table 2
Likelihood of click fraud vs. app characteristics.

DV: mean daily fraudulent rate	Col. 1	Col. 2
Intercept	0.2008***	0.1831***
	(0.0253)	(0.0372)
$Log(M\_Authentic_i)$	−0.0038	0.0043
	(0.0034)	(0.0054)
$CV\_Authentic_i$	−0.0062***	−0.0083***
	(0.0022)	(0.003)
$I(N\_Review_i > 0)$	−0.0198	−0.0930***
	(0.0181)	(0.0268)
$I(N\_Review_i > 0) \times log(N\_Review_i)$	0.0031	−0.0018
	(0.0022)	(0.0032)
$I(N\_Review_i > 0) \times M\_Rating_i$	0.0003	0.0101
	(0.0044)	(0.0065)
$Log(N\_App\_Parent_i)$	−0.0014	0.0105*
	(0.0025)	(0.0054)
$Category_i$ (Entertainment)	−0.0298***	−0.0050
	(0.0082)	(0.0488)
$Category_i$ (Entertainment) × $Log(M\_Authentic_i)$		−0.0122*
		(0.0069)
$Category_i$ (Entertainment) × $CV\_Authentic_i$		0.0045
		(0.0043)
$Category_i$ (Entertainment) × $I(N\_Review_i > 0)$		0.1170***
		(0.0361)
$Category_i$ (Entertainment) × $I(N\_Review_i > 0) \times \log(N\_Review_i)$		0.0069
		(0.0043)
$Category_i$ (Entertainment) × $I(N\_Review_i > 0) \times M\_Rating_i$		−0.0172**
		(0.0087)
$Category_i$ (Entertainment) × $Log(N\_App\_Parent_i)$		−0.0154**
		(0.0060)
$Category_i$ (Social)	−0.0233	0.3717
	(0.0328)	(0.4986)
$Category_i$ (Social) × $Log(M\_Authentic_i)$		−0.0625
		(0.0714)
$Category_i$ (Social) × $CV\_Authentic_i$		−0.0132
		(0.0305)
$Category_i$ (Social) × $I(N\_Review_i > 0)$		−0.0172
		(0.3308)
$Category_i$ (Social) × $I(N\_Review_i > 0) \times log(N\_Review_i)$		0.0388
		(0.0434)
$Category_i$ (Social) × $I(N\_Review_i > 0) \times M\_Rating_i$		−0.0170
		(0.0684)
$Category_i$ (Social) × $Log(N\_App\_Parent_i)$		−0.0366
		(0.0530)
N. of obs.	706	706
R^2	0.0322	0.0868

***$p < 0.01$, **$p < 0.05$, *$p < 0.1$. In column 2, the baseline is utility apps.

mean rating for app i before day t, and μ_i and τ_t are fixed effects for the app and day, respectively. The other variables are defined the same as in Eq. (1).

We report the results in Table 3. The results in column 1 show that on average the daily number of fraudulent clicks are positively correlated with that of the authentic clicks. This is consistent with the empirical pattern in the data. For each app, we calculate the correlation between the daily number of fraudulent and authentic clicks during the data period. We find that almost all the correlations are positive (only six of 706 apps have negative correlations). The results in column 2 suggest that the correlation seems irrelevant from most app characteristics, except for some review and category variables. For example, on average the correlation is lower for apps with review. However, the ones with higher ratings show greater correlations. Finally, the correlation is smaller for entertainment apps.

5.3.2. Correlation between likelihood of click fraud and the number of authentic clicks

For each app, we examine the correlation between its daily percentage of fraudulent clicks and the concurrent number of authentic clicks, after controlling for the app and time fixed effects. We run the following regression at the app-day level:

$$Fraudrate_{it} = \beta \cdot log(Authentic_{it}) + \mu_i + \tau_t + \epsilon_{it} \quad (3)$$

where i denotes the app, t denotes the day, $Fraudrate_{it}$ is the ratio of fraudulent clicks to total clicks for app i on day t, $Authentic_{it}$ denotes the number of authentic clicks for app i on day t, and μ_i and τ_t are fixed effects for the app and day, respectively.

Table 3
Correlation between daily numbers of fraudulent and authentic clicks.

DV: $Fraud_{it}$	Col. 1	Col. 2
$Authentic_{it}$	0.2243***	−0.1192
	(0.0557)	(0.3103)
$Authentic_{it} \times Log(M\_Authentic_i)$		0.0459
		(0.0369)
$Authentic_{it} \times CV\_Authentic_i$		−0.0229
		(0.0328)
$Authentic_{it} \times I(N\_Review_{it} > 0)$		−0.3214*
		(0.1882)
$Authentic_{it} \times I(N\_Review_{it} > 0) \times \log(N\_Review_{it})$		0.0133
		(0.0193)
$Authentic_{it} \times I(N\_Review_{it} > 0) \times M\_Rating_{it}$		0.0812*
		(0.0458)
$Authentic_{it} \times Log(N\_App\_Parent_i)$		0.0045
		(0.0255)
$Authentic_{it} \times Category_i$ (Entertainment)		−0.1272*
		(0.0742)
$Authentic_{it} \times Category_i$ (Social)		0.0022
		(0.0761)
App fixed effect	Y	Y
Day fixed effect	Y	Y
N. of obs.	13,570	13,570
R^2	0.8970	0.9156

***$p < 0.01$, **$p < 0.05$, *$p < 0.1$. Notes: Standard errors are clustered at the app level.

We report the results in Table 4. The daily likelihood of fraud is negatively correlated with the daily number of authentic clicks, suggesting a decreasing likelihood of commiting fraud when the current authentic traffic is higher.

5.4. Does the likelihood of click fraud exhibit temporal variations?

There are a couple of reasons that fraudsters could vary their likelihood of committing fraud over time. First, apps are paid by piece rate. If the ad price varies temporarily, fraudsters may react to that and act temporarily in return. However, the ad price mostly depends on the match between the ad and the targeted user groups, which may not exhibit clear temporal patterns. Another possibility is that fraudsters simply alternate their strategy by committing fraud on some days and no fraud on other days.

In Eq. (3), we also estimate the day fixed effects during the data period. The effect size of these estimates is small (from –0.0063 to 0.0048), and more than half of them are statistically non-significant. We plot these estimates with the lower and upper 95% confidence intervals in Fig. 2 to uncover any patterns. As most of the estimates are non-significant, the only notable observation from the figure is that there are several days in the middle when the likelihood of fraud is significantly low. Given the short sample time, however, this finding is not conclusive.

5.5. Summary of fraudster's behavior

Our findings show that apps with stable traffic generally have greater likelihood of click fraud. It also reveal how fraudsters conceal the click fraud in apps. In general, they make click fraud propotional to the daily authentic clicks. To avoid to be detected, they will lower the ratio of click fraud on the high-traffic days. This implies a concave relationship between daily click fraud and the authentic traffic. This behavior is relatively homogenous across apps, independent from most observable app charateristics. Finally, the likelihood of click fraud doesn't exhibit clear temporal pattern.

6. Empirical analysis: Agent campaign data

6.1. Sample for analysis

The agent campaign data consist of 905 campaigns executed by 95 agents, with 56,613 campaign-day observations. We first exclude two types of outliers from our data. First, some campaigns have an extremely high fraud rate, with the average daily fraud rate greater than 0.99. These campaigns account for less than 0.1% of the total authentic activations and 2.2% of the total fraudulent activations during the sample period. Second, some campaigns have less than 10 daily observations. These campaigns account for 0.3% of the total authentic activations and 1.5% of the total fraudulent activations. Thus, we have a sample of 701 campaigns from 83 agents, with 55,135 campaign-day observations.

Table 4
Likelihood of click fraud vs. the number of authentic clicks.

	DV: $Fraudrate_{it}$
$Log(Authentic_{it})$	-0.0140^{***}
	(0.0020)
App fixed effect	Y
Day fixed effect	Y
N. of obs.	13,570
R^2	0.9429

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$. Notes: Standard errors are clustered at the app level.

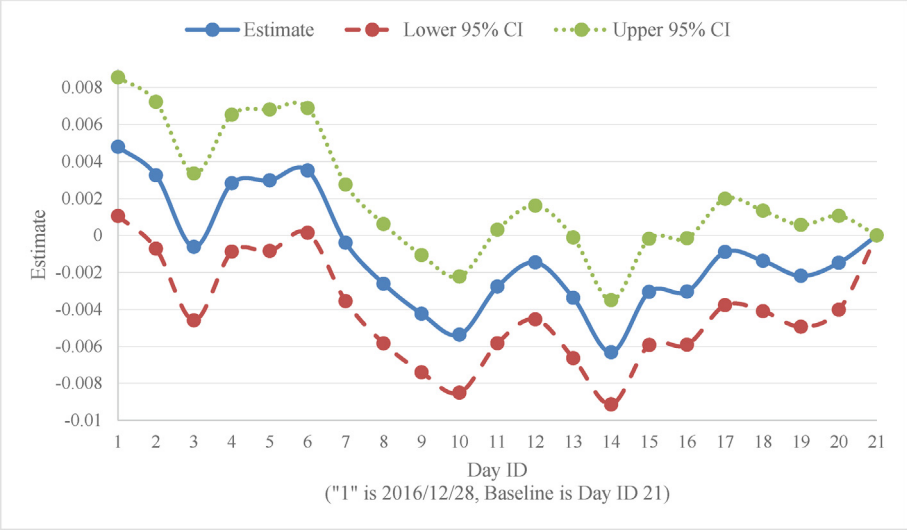

Fig. 2. Temporal effect of app's click fraud. Note: The solid line represents parameter estimates, the dashed line shows the lower 95% confidence interval, while the round-dot line depicts the upper 95% confidence interval.

Unlike app cases in which the contract has no time limit, the agent campaign data has a clear contract length for each campaign. However, not all the campaigns in our sample have complete observations. Some campaigns have observations on the first day of the data period, while others have observations on the last day. In both cases, the observations for these campaigns could be incomplete (i.e., they may have started before or ended after the data period), but we cannot verify this given the lack of contract information. This poses a potential challenge for our analysis. If a temporal effect exists during the campaign period (one of the questions we examine), all our analyses could be affected. For example, the calculated average fraud rate of a campaign will be biased if a temporal effect exists and campaign observations are incomplete. For the same reason, the estimated correlation between numbers of fraudulent and authentic activations will also be biased. Finally, if we do not observe the complete campaign period, it is not possible to study the temporal effect of ad fraud during the campaign period. There is no obvious solution to this data truncation problem because we have little information about the rule of this truncation. Therefore, we exclude campaigns with incomplete observations. This leaves us a final sample of 339 campaigns from 45 agents, with 19,358 campaign-day observations.

For each campaign, we calculate the aggregate measurements and report the summary statistics across all campaigns in Table 5. On average, each campaign lasts for 57 days, with a minimum of 10 days and a maximum of 330 days. Each campaign generated 34,200 authentic activations on average, with 440 activations on a daily basis. The variation of daily authentic activations is modest, with a coefficient of variation of 0.70. The average daily fraud rate, or the ratio of fraudulent activations to daily total activations, is 26%.

6.2. Does the likelihood of fraudulent activation correlate with campaign features?

Our approach in this analysis is similar to that for the publisher data. However, the information regarding campaigns is limited in this case. We treat each campaign as one observation to examine the relationship between the likelihood of fraud-

Table 5
Campaign-level summary statistics for the agent campaign data.

Variable	*Mean*	*SD*	*Min*	*Max*
N. of observations	57.10	53.04	10.00	330.00
Total authentic activations (10^4)	3.42	7.67	0.00	68.92
Mean daily authentic activations (10^3)	0.44	0.67	0.00	9.74
Coefficient of variation of daily authentic activations	0.70	0.50	0.08	4.67
Mean daily fraudulent rate	0.26	0.31	0.00	0.99
Corr(daily authentic activations, daily fraudulent activations)	0.27	0.53	−1.00	1.00
Campaign length (month)	2.91	2.39	0.33	12.00

ulent activations and campaign features, including the ability to attract authentic activations and contract length. Specifically, we run the following regression:

$$Fraudrate_{ij} = \beta_1 \cdot log(M\_Authentic_{ij}) + \beta_2 \cdot CV\_Authentic_{ij} + \gamma \cdot C\_Length_{ij} + \theta \cdot \sum_{k=1}^{11} Month_{ijk} + \mu_i + \epsilon_{ij}, \quad (4)$$

where i denotes agent, j denotes campaign executed by agent i, and $Fraudrate_{ij}$ is the ratio of fraudulent activations to total activations in campaign j run by agent i. Similar to before, $M\_Authentic_{ij}$ is the mean and $CV\_Authentic_{ij}$ is the coefficient of variation of the authentic activations, and C_Length_{ij} is the contract length in months, all for campaign j run by agent i. We also control for seasonality by using the variable $Month_{ijk}$, which captures the percentage of days in month k when campaign j is running. For example, if a campaign runs through the whole month of January and half the month of February, $Month_{ij1}$ equals 1, $Month_{ij2}$ equals 0.5, and the rest of $Month_{ijk}$ equals 0. Finally, because agents typically run multiple campaigns, we also include the agent fixed effect μ_i to control for the agent-specific effect on the likelihood of ad fraud.

To control for the agent fixed effect in the analysis, we exclude agents with only one campaign in our data, which results in eight campaigns being dropped. We report this analysis in Table 6. The results show that the likelihood of fraudulent activation is negatively correlated with the mean but positively correlated with the variation of daily authentic activations. This suggests that campaigns more capable of generating authentic activations (i.e., greater mean and smaller variation of daily authentic activations) have less fraud. Moreover, longer campaigns have less fraud.

6.3. Do fraudulent activations correlate with the number of authentic activations?

Similar to the app data, we decompose this question into two sub-questions. The first is whether the number of fraudulent activations correlate with that of authentic activations. If so, what observable factors explain the correlation? The second is whether the likelihood of fraudulent activations correlates with the numebr of authentic activations.

6.3.1. Correlation between numbers of fraudulent and authentic activations

We regress each campaign's daily number of fraudulent activations onto its daily number of authentic activations, while interacting with campaign features:

$$Fraud_{jt} = \left[\beta_0 + \beta_1 \cdot log(M\_Authentic_j) + \beta_2 \cdot CV\_Authentic_j + \beta_3 \cdot C\_Length_j\right] \cdot Authentic_{jt} + \mu_j + \tau_t + \epsilon_{jt}, \quad (5)$$

where j denotes the campaign, t denotes the day, $Fraud_{jt}$ is the daily number of fraudulent activations and $Authentic_{it}$ is the daily number of authentic activations, both in campaign j on day t. $M\_Authentic_j$ is the mean and $CV\_Authentic_j$ is the coefficient of variation of the authentic activations, and C_Length_j is the contract length in months, all for campaign j. Finally, μ_j and τ_t are fixed effects for the campaign and day, respectively.

We report the results in Table 7. The results in column 1 show that on average the daily number of fraudulent activations are positively correlated with that of the daily authentic activations. However, the results in column 2 suggest that the correlation is smaller for campaigns with longer period and more capable of generating authentic activations (i.e., greater mean of daily authentic activations) but unstable (i.e., greater variation of daily authentic activations). This is consistent with the empirical pattern in the data. For each campaign, we calculate the correlation between the numbers of fraudulent and authentic activations. In contrast with the publisher data, though a positive correlation still dominates, 97 of 339 campaigns exhibit negative correlations. Among these 97 campaings, many have moderate mean and large variation of daily authentic activations.

6.3.2. Correlation between likelihood of fraudulent activations and the number of authentic activations

For each campaign, we examine the correlation between its daily percentage of fraudulent activations and the concurrent authentic ones, after controlling for the campaign and time fixed effects. We run the following regression at the campaign-day level:

$$Fraudrate_{jt} = \beta \cdot log(Authentic_{jt}) + \mu_j + \tau_t + \epsilon_{jt}, \quad (6)$$

Table 6
Likelihood of fraudulent activations vs. campaign features.

DV: $Fraudrate_{ij}$	
$Log(M\_Authentic_{ij})$	−0.1663***
	(0.0061)
$CV\_Authentic_{ij}$	0.1317*
	(0.0665)
C_Length_{ij}	−0.0268***
	(0.0034)
Agent fixed effect	Y
Calendar month effect	Y
N. of obs.	331
R^2	0.7647

***$p < 0.01$, **$p < 0.05$, *$p < 0.1$. Notes: S.E. are clustered at the agent level.

Table 7
Correlation between numbers of fraudulent and anthentic activations.

DV: $Fraud_{jt}$	Col. 1	Col. 2
$Authentic_{jt}$	0.0373***	0.3346**
	(0.0116)	(0.1319)
$Authentic_{jt} \times Log(M\_Authentic_j)$		−0.0289**
		(0.0129)
$Authentic_{jt} \times CV\_Authentic_j$		−0.0584***
		(0.0206)
$Authentic_{jt} \times C\_Length_j$		−0.0004
		(0.0040)
Campaign and day fixed effect	Y	Y
N. of obs.	19,358	19,358
R^2	0.5266	0.5336

***$p < 0.01$, **$p < 0.05$, *$p < 0.1$. Notes: Standard errors are clustered at the campaign level.

where j denotes the campaign, t denotes the day, $Fraudrate_{jt}$ is the ratio of fraudulent activations to total activations for campaign j on day t, $Authentic_{jt}$ denotes the number of authentic activations for campaign j on day t, and μ_j and τ_t are fixed effects for the campaign and day, respectively.

We report the results in Table 8. The daily likelihood of fraud is negatively correlated with the numebr of authentic activations, which is similar to the findings in the publisher data.

6.4. Do fraudulent activations exhibit temporal variations?

Given the contract length and the requirement of a minimum number of activations in the campaign, we investigate whether fraudulent activations are distributed uniformly along the campaign period. If not, could they be front-loaded or back-loaded during the campaign period? Or, could the fraudulent activations be more prevelant if the recent authentic traffic is lower than usual?

To examine this, we run the following regression:

$$Fraudrate_{jt} = \beta_1 \cdot log(Authentic_{jt}) + \beta_2 \cdot Period\_Past_{jt} + \beta_3 \cdot Period\_Past_{jt}^{\ 2} + \beta_4 \cdot RecentLow_{it} + \mu_j + \tau_t + \epsilon_{jt} \quad (7)$$

where $Period\_Past_{jt}$ is the percentage of contract period that has already passed before day t for campaign j. For example, if campaign j starts on day 1 and lasts for 10 days, on day 3 ($t = 3$), $Period\_Past_{j3} = (3 - 1)/10 = 0.2$ (i.e., 20% of the contract period has passed before day 3). Conceptually, this is a state variable a fraudster would consider when making a decision on day t. The variable $RecentLow_{jt}$ captures whether the recent authentic activations is lower than usual, and is defined as the percentage change between the average authentic activation in the past seven days (denoted as a_{it}) and the average authentic activation before the past seven days since the beginning of the campaign (denoted as b_{it}), i.e., $RecentLow_{jt} = (a_{jt} - b_{jt}) / b_{it}$. When t is within the first seven days of the campaign, b_{it} is ill-defined so we set $RecentLow_{jt} = 0$ in that case. Other variables are similar to those in Eq. (6).

We report the results in column 1 of Table 9. The daily likelihood of fraud is still negatively correlated with the number of authentic activations, as we found in Eq. (6). In general, the likelihood of fraud exhibits a temporal pattern of the inverted U shape. Given that $Period\_Past_{jt}$ ranges from 0 to close to 1, the estimates suggest that the peak occurs at $Period\_Past_{jt} = 0.495$

Table 8
Likelihood of fraudulent activations vs. the number of authentic activations.

DV: $Fraudrate_{it}$	
$Log(Authentic_{it})$	-0.0993^{***}
	(0.0072)
Campaign fixed effect	Y
Day fixed effect	Y
N. of obs.	19,358
R^2	0.8100

$^{***}p < 0.01$, $^{**}p < 0.05$, $^{*}p < 0.1$. S.E. are clustered at the campaign level.

for campaigns. In other words, the extent of fraud in a campaign exhibits a mid-loaded pattern; that is, it starts low, then gradually increases until it peaks around half the campaign period, and then gradually decreases again until the end of the campaign period. Meanwhile, if the recent authentic activation is lower than before, the likelihood of fraud increases.

6.5. Summary of fraudster's behavior

Our findings shed some light on how the frausters conduct ad fraud in the advertising campaign. In general, the ad fraud is more severe in campaigns that are shorter and less capable of generating authentic activations. Similar to the app case, our findings also uncover certain ways used by the fraudsters to conceal fraud in the advertsing campaign. In most of the case, the fraudsters make the daily fraud propotional to the authentic traffic and reduce the ratio of fraud on the high-traffic days, which is similar to the app case. However, in campaigns with moderate but very unstable traffic, the fraudersters take a different strategy to smooth out the traffic using ad fraud, i.e., they make less fraud during high-traffic days but more on low-traffic days. During campaign period, the fraudsters also strategically allocate most part of fraud during the middle of campaign period, an attempt to reduce the risk of being detected.

7. Discussion

This article investigates ad fraud in the mobile advertising market. Although this issue is central in the advertising industry, extant literature provides little empirical insight into ad fraud. Using two unique datasets, we present empirical evidence of mobile ad fraud of publishers/apps and from ad agents' advertising campaigns.

7.1. Takeaways

Given our findings, what advice can we offer to the different parties in the ad ecosystem (advertisers, ad agents, ad networks, and publishers)? In general, buyers of advertising services (advertisers and ad agents) can use our findings to determine the extent of ad fraud and make decisions based on that. For example, when purchasing traffic from publishers, buyers need to be aware that publishers with a high ability to attract authentic traffic have less fraud rates, and there is a closer relationship between ad fraud and authentic traffic for these publishers, which makes it easier to deduce the scale of ad fraud. These features suggest that reputable publishers could be a safer bet in the advertising market. The most significant implications, however, may be for advertisers. As the ultimate buyers in the advertising market, advertisers often subcontract the task to ad agents. The temporal effect we found in the agent campaign data suggests the possibility of ad fraud beyond publishers, given that we find no clear temporal effect for publisher ad fraud. As such, how can advertisers choose trustworthy agents? Our results unequivocally highlight the necessity of selecting large and high-quality (in terms of generating authentic traffic) agents and signing longer contract terms. For sellers of advertising services (ad networks and publishers), though not our primary concern, our results may alarm them in terms of the features that can be used to determine their level of ad fraud, if any. As such, we hope that despite the information we provide, fraudsters begin regulating themselves.

For academic researchers, our findings reveal a hidden problem with advertising data. Given that many studies apply either publisher or agent campaign data, assessing the potential ad fraud problem is important. Our findings suggest that advertising effects could be over-estimated with publisher data. With the positive correlation between ad fraud and authentic traffic, adjusting the results by a discount factor is possible. The over-estimation could become worse though with agent campaign data, because these data potentially include ad fraud from both ad networks and publishers. Given both the positive and negative correlations between ad fraud and authentic traffic, simply adjusting the biased estimates would be challenging. The good news is that some studies already offer certain solutions to this problem. With agent campaign data used in these studies, the individuals in the sample are specifically maintained by the ad agent (Braun and Moe, 2013), are recruited to participate in the test (Bart et al., 2014), or are registered app users (Sahni and Nair, 2022). In this way, researchers ensure that the individuals in the data are real people.

Table 9
Temporal effect of fraudulent activations in advertising campaign.

DV: $Fraudrate_{it}$	
$Log(Authentic_{it})$	−0.0995***
	(0.0074)
$LifeCycle_{it}$	0.1059*
	(0.0611)
$LifeCycle_{it}^2$	−0.1070*
	(0.0590)
$RecentLow_{it}$	−0.00007***
	(0.00003)
Campaign and day fixed effect	Y
N. of obs.	19,358
R^2	0.8107

***$p < 0.01$, **$p < 0.05$, *$p < 0.1$. S.E. are clustered at the campaign level.

7.2. Legal regulation of ad fraud

Despite the considerable damage of ad fraud to the advertising market, the legal status of ad fraud is still murky. Most countries have laws that cover cybersecurity and information technology but nothing specific against ad fraud. For example, the General Data Protection Regulation in the European Union grants internet users rights over their data. German Cybersecurity laws prohibit owning or operating software with the intention of committing computer fraud. In India, the Information Technology Act of 2000 is the primary law dealing with cybercrime and electronic commerce.

The United States has the strictest law against ad fraud. The Computer Fraud and Abuse Act was enacted in 1986 and has been amended many times since. The law prohibits accessing a computer without authorization or in excess of authorization. So far, almost all ad fraud lawsuits have been successfully prosecuted in the United States. For example, in 2016, Estonian Vladimir Tsastin was accused by the U.S. government of ad fraud. Through the use of malware, Tsastin infected more than four million computers to generate fake clicks and collected over $14 million. He was sentenced to more than seven years in prison.[10]

Recent discussions on privacy concerns have led to the enactment of privacy protection laws in various countries. In addition to the European Union's General Data Protection Regulation in 2016 and the California Consumer Privacy Act in 2018, China passed the Personal Information Protection law in 2021. All these laws grant individuals the right to know about and to delete personal information collected by third parties. They also prohibit discrimination against individuals exercising their rights.

While the intention of these laws is to protect consumer privacy, they may hinder fraud detection efforts in the advertising market. As we discussed previously, many current detection methods depend on device information collected by apps registered in the ad networks, often without the notice of users. If users were to decline data collection given the privacy law, fraud detection ability would be significantly affected. Thus, balancing privacy protection and the need for ad fraud detection has become a challenging issue for policy makers.

7.3. Limitations and future research directions

Our study is not without limitations. First, as discussed previously, the ad fraud measurement in our data is determined by the in-house detection team, which is not precise. It would be worthwhile for researchers to explore how agents and publishers react to detection accuracy. If the payment and penalty information is known, in addition to the available information, they might be able to structurally estimate the actual ad fraud rate. This is a promising research area to pursue in the future.

Second, in the agent campaign data, we only include campaigns with complete observations during the data period. A potential bias from this approach is that campaigns with complete observations may differ from those with incomplete observations. Our data period is the complete year of 2016, so the campaigns with incomplete observations are those that span consecutive years. The bias would arise if a brand took a different campaign strategy toward the end of the year. Our conversations with the brand in the agent campaign data revealed that the campaign strategy did not significantly change across consecutive years, but a more thorough way to deal with this truncation problem is to have data with multiple years of observations. In that case, the calendar-day fixed effects could help control for any seasonality effects during advertising campaigns.

Third, the information in our data is somewhat limited, and additional information would help address some detailed questions. For example, we have only one brand and one compensation method (pay per activation) in the agent campaign

[10] https://www.justice.gov/usao-sdny/pr/estonian-cybercriminal-sentenced-infecting-4-million-computers-100-countries-malware.

data, which limits the generalizability of our findings. In addition, mobile ads often target users on the basis of their browsing history and whatever individual information the advertising networks possess, which could lead to price variations of ads across user groups depending on their commercial value to the advertisers. If fraudsters are strategic, this could vary their incentive to commit fraud for different ads and different user groups. Therefore, data with multiple brands and compensation methods, providing rich information on advertising and user groups, would not only help test whether fraudsters are strategic in their preference for targeting different ads and user groups but also extend the external validity of the study.

Finally, ad fraud and detection is a fast-moving area. Our data come from 2016 to 2017, but many things have changed in the last several years. For example, mobile ad spending has more than doubled, which attracts more fraudulent behavior to this market. Fraud technology has also evolved dramatically, with SDK spoofing becoming the most sophisticated fraud method. The previous generation of bots was predictable with standard attack patterns, which made differentiating them from human users easy (e.g., attacks from the same IP address, visits to a website thousands of times, spending the same amount of time on a page, performing the same simple actions). Today, bots behave differently—they hide in user devices, steal device information and mess it up, and imitate users' online behavior. All these actions put more pressure on detection technology to analyze each user by multiple parameters, which ultimately requires more human/device information and advanced models.

However, the extent of mobile ad fraud in data today may not necessarily be more severe. The present fraud rate in the market is an equilibrium outcome of the interaction between fraudsters and the detection forces. It is possible that the extent of fraud was less in the past due to the less significant market share of mobile ads, but at the same time the detection effort was also less. In a similar vein, the sophisticated fraud methods of today will also increase scrutiny of online traffic, which exerts a repression effect on ad fraud. A longitudinal study could examine the dynamic effects in this area, if any.

Funding

This work was supported by the National Natural Science Foundation of China [72222006; 71991461; 71902095].

Data availability

The data that has been used is confidential.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The first author thanks the support from the National Natural Science Foundation of China (72222006; 71991461; 71902095). The third author thanks the support from the National Natural Science Foundation of China (71972043).

References

Andrews, M., Luo, X., Fang, Z., & Ghose, A. (2016). Mobile ad effectiveness: Hyper-contextual targeting with crowdedness. *Marketing Science, 35*(2), 218–233.
Bart, Y., Stephen, A. T., & Sarvary, M. (2014). Which products are best suited to mobile advertising? A field study of mobile display advertising effects on consumer attitudes and intentions. *Journal of Marketing Research, 51*(3), 270–285.
Braun, M., & Moe, W. W. (2013). Online display advertising: Modeling the effects of multiple creatives and individual impression histories. *Marketing Science, 32*(5), 753–767.
Bruce, N. I., Murthi, B. P. S., & Rao, R. C. (2017). A dynamic model for digital advertising: The effects of creative format, message content, and targeting on engagement. *Journal of Marketing Research, 54*(2), 202–218.
BusinessofApps (2022, June 27). Ad fraud stats. https://www.businessofapps.com/ads/ad-fraud/research/ad-fraud-statistics.
Chae, I., Bruno, H. A., & Feinberg, F. M. (2019). Wearout or weariness? Measuring potential negative consequences of online ad volume and placement on website visits. *Journal of Marketing Research, 56*(1), 57–75.
Chen, M., Jacob, V. S., Radhakrishnan, S., & Ryu, Y. U. (2015). Can payment-per-click induce improvements in click fraud identification technologies? *Information System Research, 26*(4), 754–772.
Cho, G., Cho, J., Song, Y., Choi, D., & Kim, H. (2016). Combating online fraud attacks in mobile-based advertising. *EURASIP Journal on Information Security, 2016*(1), 1–9.
Fong, N. M., Fang, Z., & Luo, X. (2015). Geo-conquesting: Competitive locational targeting of mobile promotions. *Journal of Marketing Research, 52*(5), 726–735.
Haddadi, H. (2010). Fighting online click-fraud using bluff ads. *ACM Computer Communication Review, 40*(2), 21–25.
Iqbal, M., Zulkernine, M., Jaafar, F., & Gu, Y. (2017). Protecting Internet users from becoming victimized attackers of click-fraud. *Journal of Software: Evolution and Process, e1871*.
Jeziorski, P., & Segal, I. l. (2015). What makes them click: Empirical analysis of consumer demand for search advertising. *American Economic Journal: Microeconomics, 7*(3), 24–53.
Li, H., & Kannan, P. K. (2014). Attributing conversions in a multichannel online marketing environment: An empirical model and a field experiment. *Journal of Marketing Research, 51*(1), 40–56.
Li, X., Zeng, D., Liu, Y., & Yang, Y. (2011). Click fraud and the adverse effects of competition. *IEEE Intelligent Systems, 26*(6), 31–39.

Liu, B., Nath, S., Govindan, R., & Liu, J. (2014). DECAF: Detecting and characterizing ad fraud in mobile apps. In *Proceedings of the 11th USENIX symposium on networked systems design and implementation* (pp. 57-70). USENIX Association.
Loechner, T. (2019, April 24). Mobile and video are driving digital ad growth, but they're also the riskiest for ad fraud. Pixalate. https://www.pixalate.com/blog/mobile-video-driving-digital-ad-spend-growth-fraud.
Luo, X., Andrews, M., Fang, Z., & Phang, C. W. (2014). Mobile targeting. *Management Science, 60*(7), 1738–1756.
Lynch, O. (2021, October 15). Spotting SDK spoofing & mobile ad fraud. ClickCease. https://www.clickcease.com/blog/sdk-spoofing-mobile-ad-fraud.
Metwally, A., Agrawal, D., El Abbadi, A. (2007) Detectives: Detecting coalition hit inflation attacks in advertising networks streams. In *International World Wide Web Conference* (pp. 241-250). New York: ACM.
Opticks (2021, December 22). Who exactly is behind ad fraud? https://blog.opticksecurity.com/who-is-behind-ad-fraud.
Rafieian, O., & Yoganarasimhan, H. (2021). Targeting and privacy in mobile advertising. *Marketing Science, 40*(2), 193–218.
Rafieian, O., & Yoganarasimhan, H. (2022). Variety effects in mobile advertising. *Journal of Marketing Research, 59*(4), 718–738.
Rutz, O. J., & Bucklin, R. E. (2011). From generic to branded: A model of spillover in paid search advertising. *Journal of Marketing Research, 48*(1), 87–102.
Sahni, N. S. (2016). Advertising spillovers: Evidence from online field experiments and implications for returns on advertising. *Journal of Marketing Research, 53*(4), 459–478.
Sahni, N. S., & Nair, H. S. (2022). Sponsorship disclosure and consumer deception: Experimental evidence from native advertising in mobile search. *Marketing Science, 39*(1), 5–32.
Statista (2022). Mobile advertising and marketing worldwide - statistics & facts. https://www.statista.com/topics/5983/mobile-marketing-worldwide/#dossierKeyfigures.
Stitelman, O., Perlich, C., Dalessandro, B., Hook, R., Raeder, T., Provost, F. (2013) Using co-visitation networks for detecting large scale online display advertising exchange fraud. In *Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*.
Wilbur, K., & Zhu, Y. (2009). Click fraud. *Marketing Science, 28*(2), 293–308.
Zhang, L., Guan, Y. (2008) Detecting click fraud in pay-per-click streams of online advertising networks. In *Proceedings of the 28th International Conference on Distributed Computing Systems.*
Zhang, Q., Ristenpart, T., Savage, S., & Voelker, G. (2011) Got traffic? An evaluation of click traffic providers. In *Proceedings of the 2011 joint WICOW/AIRWeb workshop on web quality* (pp. 19-26). Association for Computing Machinery.
Zubcsek, P. P., Katona, Z., & Sarvary, M. (2017). Predicting mobile advertising response using consumer colocation networks. *Journal of Marketing, 81*(4), 109–126.