AdAge

COMBATING AD FRAUD IN THE AGE OF COVID-19

Sponsor Content

SPIDER AF

iStock

COMBATING AD FRAUD IN THE AGE OF COVID-19

As demand for online content has increased, so have digital ad budgets—and opportunities for fraud. The solution is a multi-tiered industry-wide initiative.

The impact of the COVID-19 pandemic has been profound and far-reaching. As of the last week of October, 45.3 million individuals globally had been infected, with more than 1.1 million deaths reported. At the same time, the global economy has been crippled and the list of industries to be adversely affected by the coronavirus is long. From airlines, restaurants and hotels to manufacturing, retail and entertainment, the virus continues to wreak havoc on the companies and their workers worldwide.

Brand marketing has also been turned upside down, and as the business of advertising has been disrupted, fraudsters—the bêtes noires of the ad industry long before COVID—have enjoyed boom times.

First, the digital domain overall has seen a marked increase in fraud since the coronavirus first emerged. Global quarantining policies have meant millions of people transitioning to remote working. The shift was sudden, leaving some companies unable to adopt proper security measures and making them all the more vulnerable to cyberattacks. Institutions from Twitter to the World Health Organization have been hit.

Along with the rise in scams like ransomware, trojan viruses and malware, ad fraud has also spiked dramatically. As traditional forms of marketing have been negatively impacted—for example, outdoor and transit ads, which have suffered from a decline in daily commuting and foot traffic—brands have shifted their budgets to digital advertising, a market that was already experiencing dramatic growth and, along with it, an explosion in fraud-related activity.

"With quarantining, there has been a huge demand for online content. Also, there are a lot of people out of work—and that includes criminals," says Rachel Nyswander Thomas,

COO of the global anti-fraud initiative the Trustworthy Accountability Group (TAG). Thomas noted that fraudulent activity TAG used to notice happening mainly on weekends has now become a 24/7 industry.

TAG was formed by the largest ad industry trade groups in the U.S. six years ago, at a time when the business was losing $8.2 billion annually to fraud. Today, according to Thomas, campaigns bought through a TAG-certified channel have reduced the rate of fraud anywhere from 88% to 94%. TAG's nearly 700 members include the world's largest brands, agencies, publishers and ad tech companies—including Amazon, Disney, NBCUniversal and Omnicom Group.

A global issue

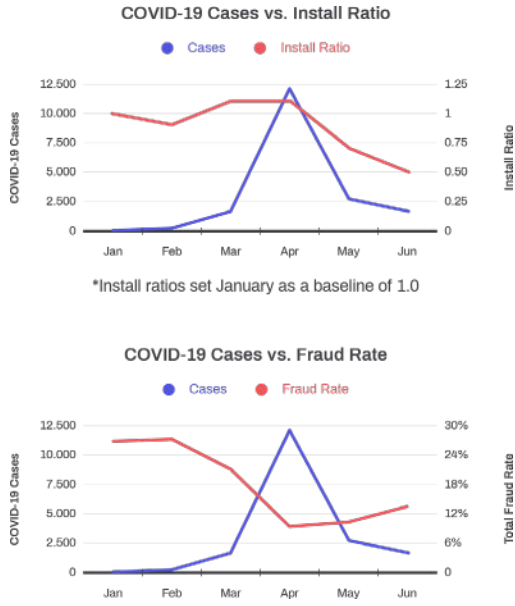
Like the coronavirus itself, ad fraud is a global phenomenon, independent of borders. In the U.S., major tech and media players have grappled with the issue. For example, Google has been closely monitoring advertiser behavior since the earliest days of the pandemic, forming a COVID-19 task force that, the tech giant maintains, "has improved existing enforcements systems and created new detection technology." Google reported blocking and removing tens of millions of COVID-related ads for policy violations including price-gouging, capitalizing on global medical supply shortages, making misleading claims about cures and promoting illegitimate unemployment benefits.

As early as March, when the pandemic was just beginning to rear its head in the U.S., Ad Age reported that The New York Times had started blocking questionable ads related to COVID, specifically those hawking N95 masks, which at the time were in short supply among medical professionals and which the surgeon general urged the general public not to buy. The Times went on to shut off all programmatic ads for its COVID newsletter, as such ads can be difficult to police. "Bad actors will see the opportunity and capitalize on it," Marc Goldberg, chief revenue officer at brand safety firm Method Media Intelligence, told Ad Age. "The underbelly is opportunistic."

The following month, Ad Age reported that the U.S. Federal Trade Commission (FTC) had hunted down several marketers of phony coronavirus cures running on Instagram and Amazon, sending them warning letters. The FTC also published on its homepage a series of tips to avoid COVID-related scams, urging consumers to be wary of emails claiming to be from WHO or the Centers for Disease Control (CDC), to hang up on robocalls and to be skeptical of ads for virus-testing kits. Also in April, Facebook filed a lawsuit against the founder of software company LeadCloak claiming it ran deceptive ads on its platforms, including bogus information about COVID.

By late September, more than 200,000 fraud-related complaints had been filed with the FTC, which reported that Americans had lost more than $145 million due to fraudulent activities related to the pandemic, according to The New York Times.

COVID-19 in Japan (cases vs. ad fraud)
COVID-19 persisted in Japan throughout most of 2020



Source: Spider Labs 2020 First Semester Ad Fraud White Paper

Impact in Japan

The other side of the coin is Japan, where COVID has impacted the population far less than in the U.S. and many other countries, including India, Russia and China. As of the second week of October, Japan had recorded a total of 87,000 cases and more than 1,600 deaths—a small number relative to the

country's total population of 126 million. And yet, ad fraud in Japan has grown by global proportions, with scams becoming more prevalent, more advanced and more damaging to the industry.

A snapshot of the market: From mid-March through April, Japan saw its first-half peak of COVID infections. Along with a surge in coronavirus cases came a significant decrease in aggregate app install rates. Likewise, rates of fraud enjoyed a brief slowdown in April and May, likely because of sudden, reactionary shifts in marketing budgets and targets as the market responded to events around the pandemic. But as coronavirus cases returned to more manageable rates, fraud rates began to rise, while installs remained low due to advertisers remaining hesitant to spend.

Amid the pandemic, the Japanese market has been plagued by a number of methods popular among fraudsters. They include:

• **Click farms.** In this scheme, a group of typically underpaid workers are hired to click on paid ads for a click farmer. (Increasingly, the work is done by bots.) Click farms can engage in deeper-funnel conversions such as installing apps, signing up for promotions, liking content and reviewing products and apps. It is difficult to detect this type of fraud, as the behavior is similar to that of legitimate users.

One of the busier groups of fraudsters is the Chinese Wool-Pulling Party, also known as the Wool Party, which overnight can pull in more than 540,000 yuan (about $80,000) via promotional tools like coupons, gift certificates and cash rewards. Members of the Wool Party are tech-savvy young people who share information on which companies to target next. (The term originates from a '90s TV drama in which an old woman working at a ranch stole the wool of a sheep to make a sweater for her husband.)

In the first half of 2020, 11.3% of clicks in the Japanese market were the result of click farms. Early Q1 click farm rates were similar to those in Q4 of last year. This year, the rates dropped in April, correlating to the rise in COVID-19 cases but slowly began growing again by Q2.

• **Click flooding.** Here, networks or publishers send a large number of clicks from real devices in an attempt to capture last click attribution. Click flooding generally includes fake clicks generated by users who did not actually click on the ad. In many cases, the ad is not even visible on the site or in the app. The goal of click flooding is to steal attribution credit for free organic installs or other networks. This is also referred to as click stuffing, cookie stuffing or click spamming.

One of the busier groups of fraudsters is the Chinese Wool-Pulling Party, tech-savvy young people who share information on which companies to target next. Overnight, members can pull in more than 540,000 yuan (about $80,000) via promotional tools like coupons, gift certificates and cash rewards.

iStock

Some examples of how click flooding can occur include hidden click elements, ad units that automatically generate a click in the background, click trackers appended to ad impressions, and fraudulent background utility apps that can generate clicks anytime. In the first half of the year, 7.2% of clicks were attributed to click flooding. As with click farming, a decline in rates in April correlated to the pandemic.

• **Domain spoofing.** In addition to combating fraud in mobile app ads, Spider Labs has expanded the battle to the domain of web advertising, where fraud based on invalid traffic is the main culprit. One of the more popular schemes is domain spoofing, a fraudulent method of earning ad dollars by falsifying referral data of an ad served. In its analysis of data from web advertisers, the firm found that domain spoofing accounted for nearly 10% of clicks on some networks.

Bogus installs

One need only examine the number of bogus mobile app installations to understand how problematic the situation is. In the first half of this year, 7.7 million app installs in Japan, accounting for 18.5% of total installs, were found to be fraudulent, according to a study produced by Spider Labs, developer of the anti-ad-fraud tool Spider AF.

The categories of apps that have been most affected:

• **Lifestyle.** The volume of installs for lifestyle apps fell dramatically between March and April, and remained sluggish throughout the first half of the year. The assumption: Increased pressure to limit social interactions during initial lockdown recommendations was to blame.

• **Gaming and comics.** These apps saw moderate increases in installs in the months of March and April, likely driven by the increase in free time among younger demographics. Japan's school year typically ends in March with the new term commencing in April, but because of COVID-19 restrictions, the spring break in between lasted until June in most of the country.

• **Dating.** These apps showed slight increases in installs, potentially due to lockdown restrictions limiting traditional forms of meeting people. Additionally, a new online dating service launched, steadily growing in popularity since April.

Joining forces

The ad industry in Japan has worked to aggressively combat ad fraud in the age of coronavirus, with disparate players joining forces to tackle the issue.

This year, the Japan Advertisers Association (JAA) invited five firms, including Spider Labs, to join with its Web Advertising Bureau to help find solutions for ad fraud. The JAA partnered with two other groups, the Japan Advertising Agency and Japan Interactive Advertising Association, to combat fraud and address other issues of import to the industry.

Since its launch in 2017, Spider Labs has aimed to provide ad fraud support for ad networks, agencies and advertisers alike, and that service across the supply chain is part of what makes it unique among competitors. Its premier product, Spider AF, detects ad fraud by analyzing data logs for impressions, clicks and conversions and events. Each media company is analyzed for signs of ad fraud and an overall ad fraud score is calculated. Of course, fraud is not limited to the domain of mobile.

In June of this year, Spider Labs launched its Web Advertisers service, diversifying its ability to fight ad fraud from multiple angles and designed to work best with Google Ads—blocking fraud and automatically adding blacklisted IPs and domains in Google Ads. The company plans to add user-level blocking by the end of 2020.

The impact of fraud on the ad industry in Japan is serious. In the first half of 2020, Spider AF calculated that 18.5% of ad data were due to fraud, taking into account 741 billion total impressions, 54 billion clicks and 42 million conversions.

As if the problem of fraud weren't enough, ad spending in Japan has struggled to recover since COVID-19 first shook the country in March and April. (In mid-April, the government declared a nationwide state of emergency.) Spend in May and June continued to be off, attributed to advertisers' hesitance

to increase budgets in an unpredictable economy.

Meanwhile, the lockdowns and other restrictions caused dramatic shifts in the app market in the country—with volumes in certain categories plummeting while others soared.

Blacklist and whitelist

In another example of how the Japanese ad industry came together to fight fraud, two years ago Spider Labs launched the Shared Blacklist (SBL), the first shared, multi-operator blacklist of its kind in the Japanese market. The SBL can be accessed by companies that have agreed to share the threat information they have obtained using Spider AF. An SBL member can see which media have been labeled as ad fraud or market as a threat to brand safety by other members.

There are limits to what a company can do alone, naturally, and SBL is one of the collaborative initiatives that has made the Japanese market uniquely positioned to fight ad fraud. As the number of companies that are part of the SBL grows, Spider Labs has vowed to work with its partners to improve the safety of the digital ad business.

The SBL has the firm backing of members of the Japanese ad industry. Some testimonials from those whose companies have signed on:

"We will create an environment in which advertisers can place ads with peace of mind." —Makota Tsunekane, manager, ad platform division, Axel Mark

"Until recently, companies have been working on combating ad fraud independently. But with Shared Blacklist, it is possible to work with a sense of solidarity as an entire industry." —Shunsake Kawasaki, executive officer, GENIEE

"In the past, we eliminated fraudulent traffic just for ourselves, but from now on, we want to help clean up the industry and provide ads that are valuable to advertisers and users." —Sho Yamada, CEO, Unicorn

"It's time for advertisers, publishers and ad platforms to not only be aware of ad fraud but also take action to make digital advertising safer." —Koji Ninomiya, director, Fancom

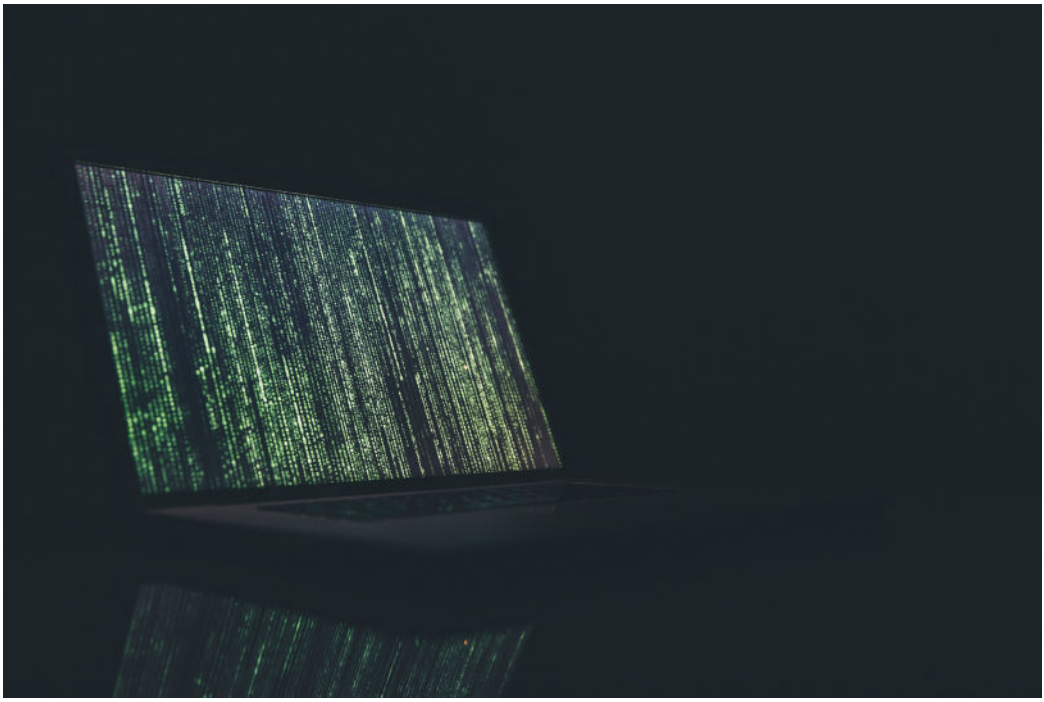
Even though there's strength in numbers, there are still challenges to combating fraud—among them, privacy laws. Much attention was paid to the implementation, in May 2018, of the European Union's General Data Protection Regulation (GDPR), which sought to enable the movement of personal data within the EU while protecting the rights of individuals. (The EU has included Japan on its "whitelist" of countries it has deemed have an adequate level of personal data protection.)

And yet, the Japanese Act on the Protection of Personal Information dates all the way back to April 2005. A reformed version went into effect in May 2017—a full year before GDPR—that included a white list similar to that of the EU. Since then, the establishment of Japan's Personal Information Protection Commission, which establishes and enforces privacy laws, "significantly enhances Japan's privacy law system," Kensaku Takase of the firm Baker McKenzie, and member of the International Association of Privacy Professionals (IAPP), stated in a report published by the association.

Meanwhile, in the U.S., in contrast to the EU and Japan, there remains no overarching legislation, even though a patchwork of federal and state laws aim to protect consumers' data and privacy.

With an estimated 20% of ad budgets globally being snatched by fraudsters, marketers in the U.S., the EU and other markets can learn much from Spider Labs, its Shared Blacklist innovation, and the firm's joining forces with the JAA and other groups in Japan committed to combating ad fraud—principally that by working together to identify the bad players and interrupt their plans to disrupt business, marketers can stay one step ahead of ad fraud and protect their bottom line.

The ad industry and firms like Spider Labs that specialize in battling fraud will remain especially vigilant as the coronavirus pandemic continues to upend the global ad business. "This year, COVID-19 will have a huge impact



Markus Spiske/Unsplash

Cybercriminals continue unabated through the pandemic.

on economic activity," Spider Labs CEO Satoko Ohtsuki comments. "There is still no relief in sight, and we are still forced to work remotely and conduct our business activities in a non-face-to-face manner.

"But we will continue to make even greater strides," she says, adding that the industry "must work together."

Key takeaways

• Cybercriminals are not taking a break during the coronavirus pandemic, and marketers must remain more vigilant than ever as ad fraud continues to be a global phenomenon, affecting the likes of Google, Facebook and The New York Times.

• According to Spider Labs' analysis, fraudulent activity in Japan slowed for a brief period during the peak of COVID-related lockdowns in April and May. Ad fraud used in app advertising frequently changes over short periods of time. Of 42 million installs in the first six months of the year, 18.5% of total installs were found to be fraudulent. The resulting damage was estimated at $38.5 million in the term.

• There is a limit as to what participants individually can do, so it is essential that the industry work together. One of the collaborative initiatives is the Shared Blacklist, through which information about fraud can be passed between those firms being targeted. Spider Labs is among five companies partnering with the Japan Advertisers Association's Web Advertising Bureau to help find solutions for fraud. This year, the JAA partnered with two other groups, the Japan Advertising Agency and Japan Interactive Advertising Association, to combat fraud and address other issues of import to the industry. As far as partnerships with U.S.-based anti-fraud groups go, Spider Labs works with the Trustworthy Accountability Group (TAG) and says it remains open to any potential partnerships that will lead to creating a safer advertising ecosystem.

• With an estimated 20% of global ad budgets lost to fraud, marketers can use tools like Spider AF to work as a singular industry and identify the bad players, interrupt their plans for disruption and protect the bottom line.

SMARTNEWS CASE STUDY

SmartNews, a news app based in Tokyo, has surpassed 50 million downloads since its launch in 2012. To expand brand awareness and acquire new users, it implemented ad fraud countermeasures—improving return on ad spend (ROAS) by 160%—while scaling cost-per-install (CPI) network user acquisition campaigns.

When SmartNews implemented new CPI campaigns in 2018, it experienced what appeared to be an influx of fraudulent installs that caused a sharp drop in recurring app usage a certain number of days after download, says marketing manager Takashi Amitani. "We've set up thresholds for ad fraud countermeasures with the ad agency, but analysis of our internal logs revealed that this was occurring for such a long period of time and that it couldn't be tracked on the SDK's admin dashboard," he explains. "Ad fraud accounted for nearly half of the installs we acquired through the CPI campaign, which made us realize the need for additional ad fraud countermeasures."

The app stopped running CPI campaigns that could potentially be targeted by ad fraud. There were cases where it used its partner companies' brands to promote coupons. To ensure brand safety, it distributed only through whitelisted ad networks to avoid low-quality sources.

As its user base grew, SmartNews had to deal with its reach limit and the increased frequency of ad delivery to the same users, both limited since the app only served ads in specific media. "We used to target users with a strong interest in news, but we've expanded our target audience since we launched our coupon distributions," says Amitani. "There are a lot of people who are interested in information pushed out through social media ads; that's why we wanted to test the possibilities in expanding our network and to reach the majority of those users."

SmartNews used Spider AF to uncover massive fraud.

While trialing the product Spider AF, he notes, the company found that approximately 90% of installs in a new CPI campaign were fraudulent. SmartNews not only continued using the service but encouraged its ad agency to look into the tool as well.

Amitani, who comes from the agency side, explained that SmartNews partners with agencies not for short-term cost-per-action (CPA) purposes but for medium- to long-term business growth. With that in mind, the client looks to its agency partners for activities including blacklisting media, excluding fraud from billing, and implementing ad-fraud measures. Objective metrics are key, he says, "to have data that everyone agrees is fraud."

This has enabled the firm to cut costs, scale up campaigns and deliver quality ads. The firm recalculated its CPA after eliminating fraudulent ads and found that compared with other media, ROAS, as noted, increased by 160%. It also achieved an 85% retention rate after 30 days.

What is the key to preventing ad fraud? "It's a game, so it's important to tackle the issue continuously," says Amitani. "If we don't take measures against fraud, the damage will increase because the fraudsters will know that their methods work.

SmartNews

Ad Age Studio 30
Ad Age Studio 30 helps your brand connect with an influential audience actively seeking new partners, solutions and products. Through original custom articles, thought-leadership content, events, research, webcasts, white papers, infographics and more, our end-to-end solutions help your content reach and resonate.
Studio30@adage.com

Staff:
Writer: **Tony Case**
Senior Art Director: **Jennifer Chiu**
Copy Editor: **Brian Moran**

Contact us:
James Palma
General Manager, Revenue and Client Partnerships
jpalma@adage.com

John Dioso
Editor, Studio 30
jdioso@adage.com

About Spider Labs
Spider Labs, developer of Spider AF, provides anti-ad-fraud solutions from in-app to web advertising for advertisers, ad networks, agencies and publishers. Spider AF offers real-time blocking for web advertising and detection for in-app advertising. Spider Labs Ltd. was the first vendor in Japan and APAC to be certified by Trustworthy Accountability Group (TAG), the world's leading global certification program in the digital advertising industry for ad fraud. Under the vision of "Building a Safer and Happier Future with Automation," Spider Labs hopes to provide "Wow!" experiences to everyone.
https://spider-labs.com/intl/en