FRAUDSTERS LOVE PERFORMANCE MARKETING!

Find out how they infiltrate your program so you can punch ‘em in the bot.

Impact Radius

FORENSIQ
An Impact Radius company

Introduction

Ad fraud is rampant across the entire digital and mobile ecosystem. But one area fraudsters really love is performance marketing. There are just so many ways to sneak in and steal a piece of the pie!

Using a variety of tactics from simple click farms to sophisticated botnets, these bad actors aren't just stealing your profits, they're also damaging your brand and destroying the relationships you've built with true revenue-generating partners.

If you pay partners and/or affiliates on CPA, CPI, CPL or CPC, then you need to be aware of how performance fraud happens, so that you can identify and fight it.

Why? Because eliminating fraud from your performance marketing program might just be the fastest way to increase your budget without having to fight your CFO for it.

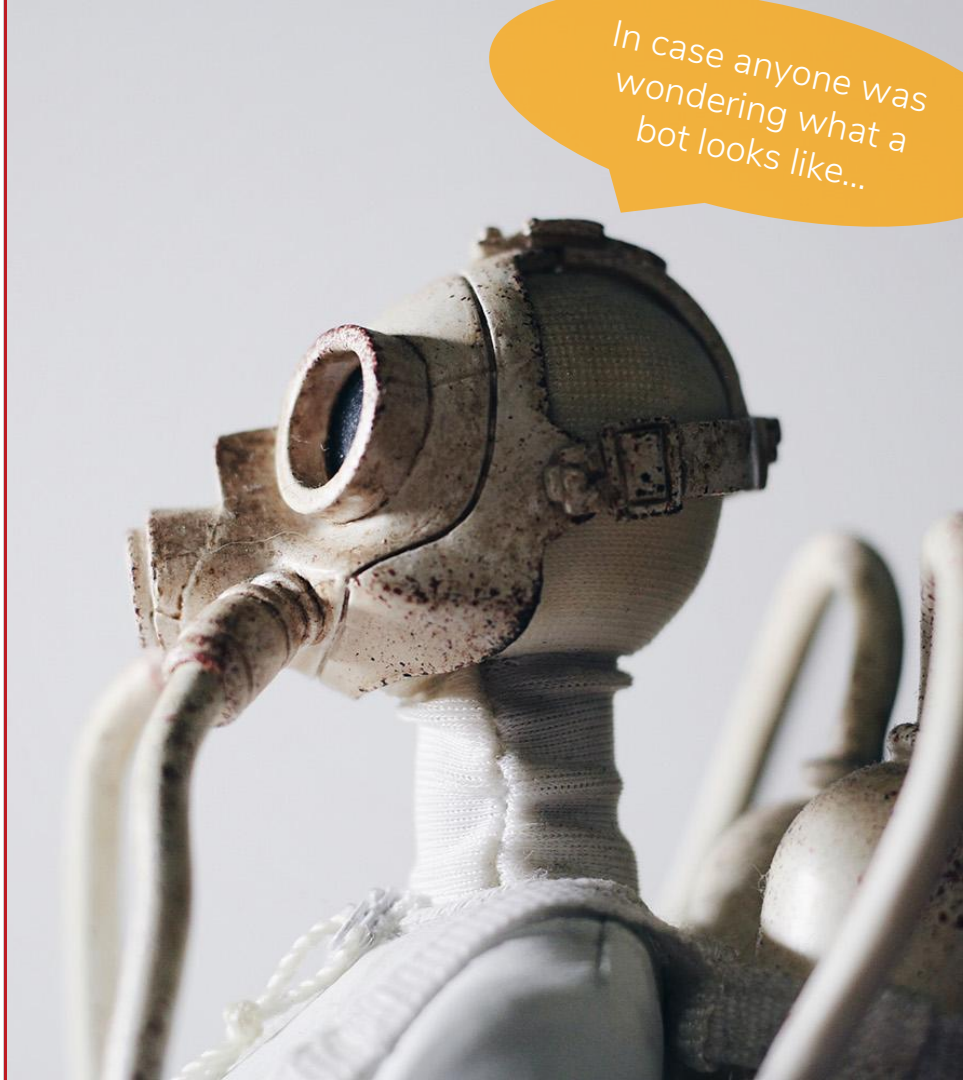
This eBook summarizes the most common types of fraud specific to performance marketing and outlines ways to combat it.

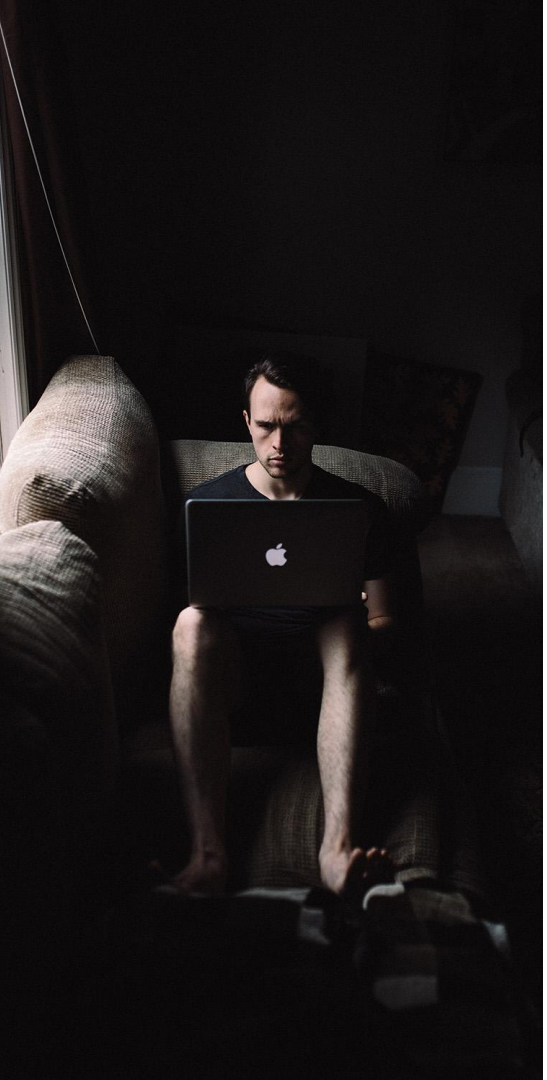
Table of contents

1.

AUTOMATED vs. NON-AUTOMATED TACTICS

Bots & fraud farms





Malicious actors can infiltrate your performance program using either automated or non-automated methods.

In an automated fashion, **bots** can mimic the behavior of legitimate humans and simulate the characteristics of legitimate browsers or devices to generate commissions via your website or mobile app.

Alternatively, fraudsters can use the coordinated efforts of real humans – **who are not real prospects** - to click ads, fill out lead gen forms, download apps or take other actions to generate unproductive commissions at your expense. These collaborations can involve thousands of low-paid workers and are aptly named click farms, form farms and install farms.

2.

MOST COMMON TYPES OF PERFORMANCE FRAUD

Cookie Stuffing, App Install & Attribution Fraud, and Lead Gen Fraud

Cookie Stuffing

When a legitimate customer clicks a legitimate ad from a legitimate partner, that partner's ID is written to a cookie, so the partner can later be paid commission for the sale.

Fraudsters use hidden iframes, browser toolbars, pop-under windows and injected ads to forcibly inject cookies and simulate clicks that never happened or were not intended by the user.

Later, if the legitimate customer converts, the bad actor is credited for the sale even though they didn't earn it.

In a similar fashion, these bad actors can fake clicks and generate a commission for traffic driven by organic referrals, making you pay for something you would otherwise have gotten for free.

App Install & Attribution Fraud

As the name suggests, malicious actors use bots to generate fake installs or use people-based install farms to download apps.

These fraudsters spoof or hijack browsers, devices and locations to virtually multiply their efforts and generate hundreds or even thousands of installs, carefully timed and executed to emulate human behavior.

As with cookie stuffing, bad actors can also steal credit for installs they did not drive. However, because attribution for app installs is cookieless, the fraudsters must create fake clicks using real device IDs and other identifiers to game the attribution.

Lead Gen Fraud

Like install fraud, bad actors use bots and/or people to generate fake form fills and earn illicit lead gen commissions.

While email or phone verification may protect lead gen marketers from less sophisticated fraudsters, the experts use advanced tactics to bypass these simple protection methods.

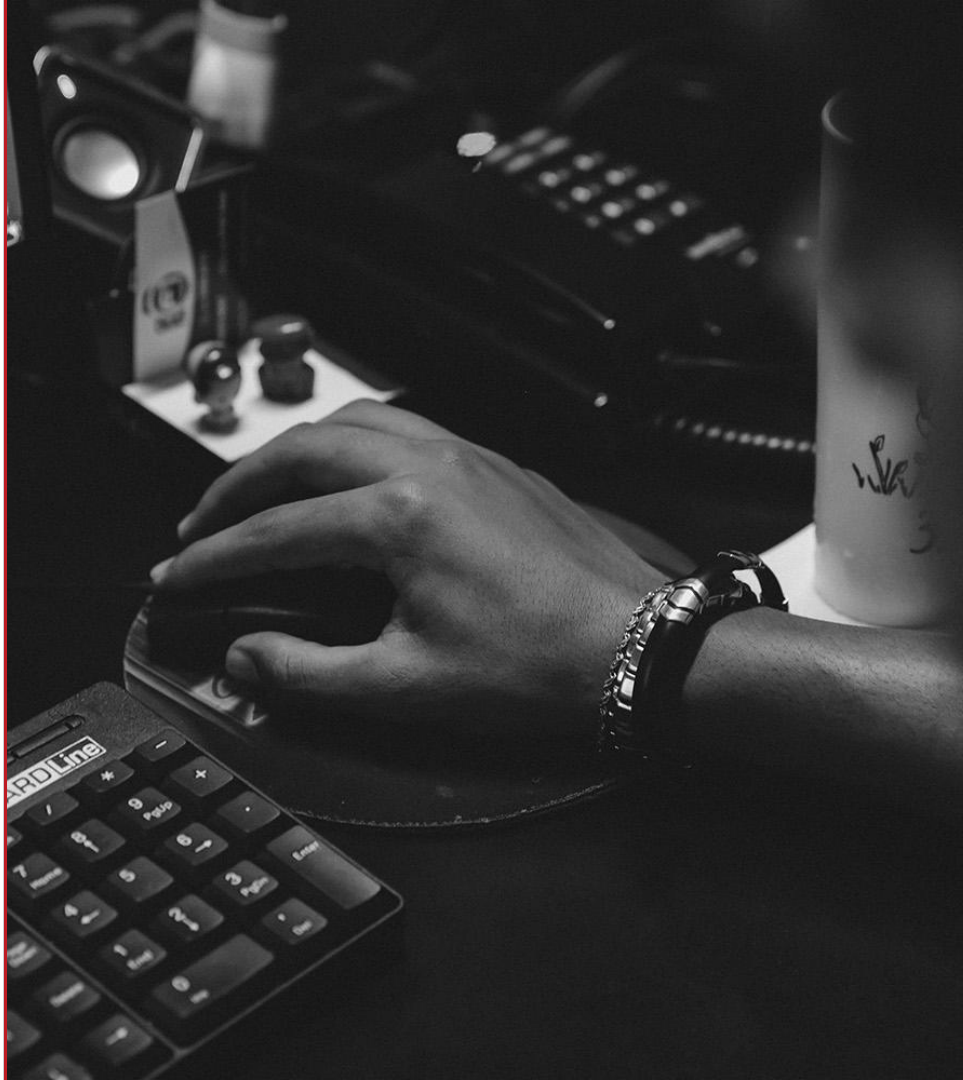
Not only is this type of fraud expensive with regards to unproductive commissions, but it's also a drain on the resources needed to validate those leads. Plus, it compromises your lead verification systems and muddies your contact database.

Worse, since fraudsters often use real contacts, it can irritate real people whose information may have been collected using other dishonest tactics and who never intended to become a prospect. As a result, these unwilling participants may feel spammed by your legitimate email and retargeting efforts, which creates an undeserved ding on your brand's reputation.

3.

DETECTING PERFORMANCE FRAUD

Manual & automated detection



Manual Fraud Detection

Fraudulent actions are often difficult to detect manually and you're limited in the types of fraud you can detect. However, there are a few reports you can create from your logs, which you can then review weekly to identify and reduce at least some fraudulent traffic.

IP Address

Multiple conversions from the same IP address are often an indication of fraud, particularly when the transactions occur in a limited window of time.

For example, 10 clicks in, perhaps, less than 3 minutes for CPC campaigns. Or 10 sales in a day for CPA campaigns. Or 5 lead gen form fills within an hour for CPL campaigns. Each can each be an indication of fraud if they come from the same IP address.

Referring URLs

Review and visit any referring URLs that seem suspicious. Does the website match the URL you have on record for that partner? Does the content of the site seem legit or does it look like a parked URL? Overall, does the site represent your brand in an acceptable way?

Be careful not to jump to conclusions. If something looks suspicious, but isn't 100% obvious as fraud, contact the referring partner to investigate.

Geolocation

Any sales, leads or other events coming from countries or regions where you don't offer products or services have the potential to be fraudulent.

On its own, geolocation is not an automatic indication, as your customer could be on vacation or living abroad. So again, be careful not to jump to conclusions.

Automated Fraud Detection

Most marketers would rather spend their time nurturing their partnerships and developing strategies to increase revenue than manually check for fraud. In fact, most marketers would probably prefer to pull out their eyelashes than manually check for fraud.

As you can imagine, reliable fraud detection platforms that automate these efforts are a welcome addition to their toolset. The platforms aren't just an enormous time saver, they are also considered more of an investment than an expense, given their innate ability to quickly reduce costs, improve efficiencies and boost ROI.

Automated fraud protection relies on a variety of methods to handle the job. The resulting reports help you to call out these bad actors, withhold payment and eliminate them from your program altogether.

Automated Fraud Detection Tool

When shopping for a fraud detection tool, be sure the technology addresses the specific types of fraud pertinent to your performance program. Also be sure the company employs ethical hackers who identify new methods of fraud and develop tactics to beat them.

Look for a tool that offers:

- Sophisticated data collection efforts to amass and process intelligence on known bad actors, so these actors are more easily recognized when they return.
- Automated traffic detection technology to identify invalid traffic from botnets, hijacked devices and malicious script injection.
- Machine-learning algorithms that identify anomalies by analyzing time and behavior patterns.
- Proxy unmasking technology to reveal fraudsters behind the IP addresses, characteristics and behaviors they hide behind.

4.

PREVENTING PERFORMANCE FRAUD

Know your partners!

Preventing Performance Fraud

Marketers can – and absolutely should – do their due diligence when choosing which affiliates and partners they allow into their program.

- Don’t put your recruiting on autopilot. Manually approve each applicant after a tangible review and a decent gut check.
- Visit the website posted in their profile. Read the content to ensure it matches what you’re selling and it doesn’t appear to be a link farm. Click through their other ads, looking for odd redirects or other unexpected or unusual behavior.
- If you are unsure of an applicant, call them on the phone to ensure they are real and to talk about your pending partnership.

Preventing Performance Fraud (cont'd)

Once your partners have officially joined your program, keep up with their efforts.

- Get to know them. Speak at least monthly via phone and at least weekly via email. Meet them in person at conferences or whenever possible.
- Work together to develop strategies and campaigns that make sense for you both. Participate in their success by providing content, creatives, copy and advice, as needed.
- Check your fraud reports (manual or from the automated tool) at least weekly to ensure things are running as smoothly as they seem and to catch issues as quickly as possible.

FRAUDSTERS ARE SMART

They constantly find loopholes and figure out new ways to take advantage of both advertisers and their customers.

To keep your brand and ROI safe, you need to keep your eye on the ball. Actively remove bad actors from your performance program as soon as you identify them and always alert your affiliate network or performance platform, so they can take the appropriate action across their ecosystem.

To learn more visit

www.ImpactRadius.com

www.Forensiq.com

Impact Radius

FORENSIQ

Together, Impact Radius and Forensiq are transforming the way advertisers handle media and performance marketing partnerships.

Our natively integrated suite of products enables digital brands and agencies to maximize their return on global ad spend by providing a single **trusted view** into the consumer journey from ad impression through acquisition across all devices and channels.