INVOCA

The Affiliate Fraud Prevention Playbook

Detect, Fight, and Prevent Affiliate Fraud to Build Trust with Your Partners

Index

A New Era of Confidence in Performance Marketing 3

What is Affiliate Fraud 4

Types of Affiliate Fraud 5

Best Practices for Preventing Fraud 9

What to do When You Suspect Fraud 11

Building Better Relationships with Fraud Fighting 12

About Invoca 13

A New Era of Confidence in Performance Marketing

Performance marketing brings brands, networks, and affiliates together to drive more traffic and conversions for brand campaigns. While many brands and performance agencies enjoy successful and mutually beneficial relationships, affiliate fraud has left the industry with a black eye.

Many say that the bad old days of shady affiliate marketing is waning, but it takes more than talk to instill confidence in your partners. In order to rebuild trust with brands and other partners, we must not only acknowledge the issues we face, but actively work to detect, fight, and prevent affiliate fraud.

The purpose of this playbook is to establish a path to preventing affiliate fraud and show brands and partners the value and stability of performance-based marketing. We will define what affiliate fraud is, breakdown the four major types of fraud, and discuss how to prevent it from impacting your business. We hope this information helps you develop quality partnerships that lead to a successful pay-per-call program.

Together, we can help fight affiliate fraud and begin a new era of confidence in performance marketing.

What is Affiliate Fraud

As you know, pay-per-call is an advertising model where an advertiser pays an affiliate commission for calls driven that meet specific conditions. These conditions can include caller region, time of call, and total talk time, as well as methods used like paid search and directory listings.

Affiliate fraud occurs when an affiliate or publisher purposely drives fake leads that violate any part of the contract in order to receive payment unjustly. This includes mimicking the advertiser's required conditions in exchange for payment or violating the allowable methods to drive traffic.

Invalid Leads vs Fraud

It is important, however, to differentiate between **affiliate fraud** and **invalid leads.** Unlike fraud, an invalid lead is simply a prospective buyer who did not or was not qualified to convert, but was driven following the advertiser's contract.

Bad leads happen to everyone and affiliates cannot be held accountable for a reasonable number of invalid leads. Since these are not malicious, the affiliate is entitled for payment.

Getting some invalid leads is normal. Make sure not to confuse them with fraud.

Types of Affiliate Fraud

Typical affiliate fraud methods come in four different but equally unsavory flavors. Let's take a look at each type and what can be done to combat them.

Unauthorized Sources

Advertisers define the acceptable media channels through which an affiliate can drive traffic. These sources may include but are not limited to:

- **Email**
- **Paid search (keyword bidding)**
- **Display**
- **Social**
- **Print ads**
- **Radio**
- **Warm transfer**

Any lead driven outside of the approved media channel is considered a fraudulent lead. While the lead may be technically legitimate, the buyer may not want leads from social, for example, and would be under no obligation to pay for them. As an example, some brands prohibit affiliates from brand name keyword bidding as it interferes with their own campaigns, so even if an affiliate drives a quality lead through that source, they should not be paid out and the call is considered fraudulent.

Stopping unauthorized sources fraud

First, you should ask all affiliates how they are driving traffic and if they're using sub-affiliates — any hesitation is a red flag. Second, make sure that you are listening to your calls to pick up on potential unauthorized sources. Lastly, you have to perform your own audits to sniff out prohibited sources. To do this, you can search for prohibited keywords and look for paid search ads that you are not posting internally, which you can then attribute to your affiliate.

Clearly state to your affiliates which sources are authorized by the buyer.

Stolen Credit Card

Stolen credit card numbers are a classic but persistent method of defrauding performance marketing customers. With a pile of stolen credit card numbers, a shady affiliate can impersonate a consumer to buy the product or service from the advertiser in order to receive a commission from the sale driven. When the real consumer disputes the charge, the credit card company reverts payment from the advertiser, but the bad affiliate keeps their payment.

This type of fraud is most prevalent in cost-per-acquisition (CPA) campaigns that require payment from the consumer before the affiliate receives a commission. It can be difficult to spot right away as it takes most advertisers 30 days to receive a dispute.By then, the affiliate will probably be gone with the wind.

Best practices to combat stolen credit card fraud

Be wary of starting CPA campaigns with new affiliates as they could be a fly-by-night operation. Leave these campaigns to established partners to avoid getting taken by surprise. You can also test a small sample of the affiliate's traffic before you go all-in to gauge the quality of their leads.

You should also keep an eye on your conversion rates. If you see a sudden spike where conversion rates are unusually high, don't start patting yourself on the back right away — it could be credit card fraud. Of course, you can also cut fraudsters off at the pass by waiting to pay them until the end of the business cycle. Fraudulent affiliates won't want to wait around to get paid and potentially caught.

Keep an eye out for sudden spikes in conversion rates — it may be credit card fraud.

Account Selling

Agreements between advertisers and affiliates are between specific organizations. If an affiliate has a good reputation, quality relationships, and solid commissions, another affiliate may want to impersonate them by buying their online accounts.

There are online marketplaces that facilitate the sale of pre-activated affiliate accounts to a specific advertiser or network. Since advertisers set up agreements with specific affiliates, buying an account to impersonate the established affiliate is a breach of conditions.

Best practices to combat account selling fraud

The best way to prevent account selling fraud is to know your affiliates well. Have regular meetings with your point of contact so you can stay on top of all your accounts. You can more easily spot red flags if you are working closely with your affiliates. While you're at it, you can both keep a close eye on new user accounts. Anything that looks unusual here should be investigated immediately. The technological solution to lock out fraudsters is to use two-factor authentication on all of your accounts.

Establishing solid relationships with affiliates and having regular meetings is one of the best ways to prevent fraud.

Mystery Shopper

Also known as incentive traffic, bad affiliates will impersonate or hire others to impersonate interested buyers in order to meet the advertiser's requirements and receive a commission. These callers sound interested, provide information, and stay on calls for believable durations.

Mystery shoppers are some of the worst offenders on performance campaigns and can be very

difficult to catch. Many of the “mystery shoppers” are hired through Craigslist ads, emails, and recruiting sites, and the people making the calls are completely unaware that they are part of a scam, so they take what they are doing seriously. Some are actually paid by the affiliate, but most figure out that they made a bad move when the check for their “mystery shopping” duties never arrives.

Best practices to combat Mystery Shopper fraud

A big red flag for a deluge of “mystery shoppers” is unusually low conversion rates. This will often happen when payment is based on call duration, so the shoppers are set up to stay on the phone for a predetermined amount of time. And, of course, they never end up buying.

Call recordings are also handy for sniffing out mystery shoppers. You want to listen for obviously scripted calls and listen for the same voice over and over again. If the same person calls saying the same thing over and over, it’s not a good call. You can also run reports on Caller IDs calling multiple campaigns within a short period of time and block them. Call tracking and analytics solutions like Invoca can automatically detect and block these calls.

A sudden drop in conversion rates might not be a mystery, it could be mystery shopper fraud. Check call recordings for telltale signs like repetitive, scripted calls.

Best Practices for Preventing Fraud

The best way to fight affiliate fraud is to prevent it from happening in the first place. Here's how to keep it at bay.

Pre-launch evaluation

Understand the vulnerability risk based on your company's vertical. Be familiar with the questions call center agents ask and listen to real caller conversions to quickly identify poor quality or fraudulent sounding calls.

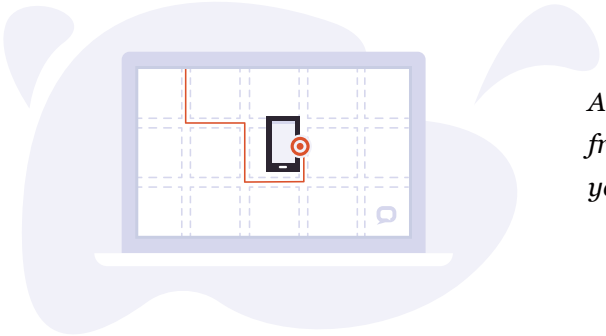
Know your affiliates

Establish a relationship and have regular meetings with the same affiliate point-of-contact. Ask to see their business website, business registration, and get references from other partners. Monitor the number of affiliate users per account, and manually approve new publisher accounts. Know how an affiliate is driving calls and if they are using sub-affiliates. Any hesitancy to share information can be a red flag.

Use the right technology

While you will always need to keep your eyes and ears open for unusual activity, technology is here to help. Advanced call tracking and analytics solutions like Invoca not only provide you with recordings of every call, but it can automatically detect and prevent fraudulent calls from ever hitting the contact centers of your customers. Invoca blocked over 2 million fraudulent calls in 2017 alone, and we work closely with law enforcement to combat fraud industry-wide. If bad calls never reach your customers, it builds trust, saves everyone time and money, and allows you to focus more on your core business.

Enabling two-factor authentication also adds another layer of security. It forces users to associate their account with a real phone number. When the account is accessed in a new location, the user cannot access the account unless they put in a one-time password sent by text. This ensures the real account contact is accessing the affiliate account.



Advanced call tracking platforms can stop fraudulent calls before they can ever reach your buyers.

Test smart

When bringing on new affiliates, start with a small budget or call cap to quickly gauge the quality of calls. If everything looks good, rock on! If something smells fishy, don't hesitate to investigate or walk away.

Review reports

You must vigilantly evaluate call volume and conversion rates for new affiliates. For established partners, you can compare volume of one period of time over another. Listen to a sample of call recordings. Conversion rates that are too good to be true or make a significant change in a short period of time should be of concern.

Be active in the industry

You can keep up with the latest trends from the dark side by participating in online Facebook groups, attending affiliate conferences, and networking with advertisers, networks and affiliates. Nobody knows the business as well as your peers.

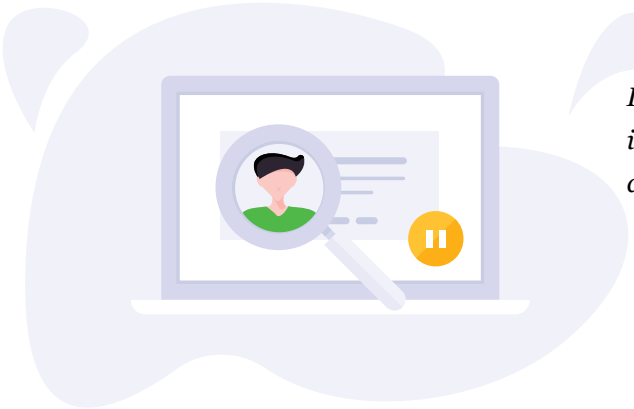
What to do When You Suspect Fraud

If after following the above steps you feel that an affiliate is committing fraud on your network, it's time to take action.

Evaluate your relationship with the affiliate and decide if you want to continue working with them. Notify them that you have discovered fraud and what your planned course of action is (terminate relationship, probation, etc.)

To temporarily or indefinitely terminate the relationship, suspend the affiliate account to stop all traffic and access. Calls to a suspended affiliate's promo numbers are not routed and commissions are not earned, and users cannot login to their account.

While it's tempting to publicly sound the alarm, be cautious about publicly posting about your suspicions about an affiliate driving fraudulent calls. If an affiliate chooses to fight back, this could lead to legal issues such as defamation. Of course, if you are using Invoca, you can also reach out to your customer success representative for assistance if you suspect fraud.



Don't jump the gun. If you suspect an affiliate is committing fraud, suspend their accounts and investigate further.

Building Better Relationships with Fraud Fighting

Given the history of fraud in performance marketing and the suspicions that brands may have about the industry, it's tempting to put your head in the sand and quietly fight the baddies. In order to rebuild the reputation of the industry and instill trust in your partners past, present, and future, it's time to face the beast head on and show that you're doing everything in your power to fight it.

Don't hide the fact that you are actively fighting affiliate fraud for fear of acknowledging its existence. Brands already know that it exists and they are wary of it, so the best way to build trust with them is to show that you and the industry in general is doing something about it. Gather any metrics you can that show you are blocking bad calls, vetting your affiliates carefully, testing your methods, and monitoring performance.

Turn your best partners into advocates with case studies and other co-marketing to display the trust that you have already built. And when you use platforms like Invoca that battle call fraud with technology, use that as part of your selling and confidence-building strategy as well.

The performance and affiliate marketing industry is in a much better place than it was just a few years ago, but there is still work to be done. Building trust with your partners by diligently fighting fraud is the big first step. Once confidence is restored, then it is much easier to show the value and ROI of performance marketing for all parties involved.

Learn More About How Invoca Fights Affiliate Fraud

Want to see how Invoca keeps affiliate fraud at bay? Schedule a demo or give us a call today.

Invoca.com/performance | **855-333-2446**

About INVOCA

Invoca is an AI-powered call tracking and analytics platform that helps marketers get campaign attribution and actionable data from inbound phone calls. Invoca delivers real-time call analytics to help marketers take informed actions based on data generated before and during a phone conversation. As a result, marketers can dramatically improve ROI by driving more revenue-generating calls, increasing conversion rates, personalizing the customer journey, and running more efficient campaigns.

With Fortune 500 customers in telecommunications, financial services, insurance, healthcare, and home services, Invoca's platform integrates with Google Marketing Platform, Facebook, Adobe Experience Cloud, and Salesforce Sales and Marketing Clouds. Invoca has raised over $60M from Accel Partners, Upfront Ventures, Morgan Stanley Alternative Investment Partners, Salesforce Ventures, and Rincon Venture Partners. For more information, visit **https://www.invoca.com**.