4 STEPS TO PREVENT AFFILIATE MARKETING FRAUD

IPQUALITYSCORE
PROACTIVELY PREVENT FRAUD

THE PROBLEM

Affiliate marketers, affiliate networks, and the industry's advertisers **lose $8.2 billion dollars** (and rapidly climbing) **per year**, and many don't realize it yet.

What's the problem?

Low quality, fraudulent traffic.

Of course, low quality and non-human traffic results in headaches such as bad relationships with advertisers, reversals and chargebacks, negative ROIs for partners, and more importantly, **fraud**.

Fraudsters utilize bots and automated scripts connected to proxies and VPNs to disguise their identity and take advantage of the affiliate industry-**but there is a way to fight back.**

This guide covers the 4 steps to fight fake traffic and fraud, as well as a guide to key terms and what to look for in a solution.

Affiliate Marketers that follow these steps will experience:

- Higher ROIs on media spend
- Better reputation within the industry
  Total dominance over competition*
- Peaceful sleep without worrying that bots and fraudsters are ravaging their traffic

*Our customers use their ability to defend traffic when pitching advertisers, so can you. Guaranteed clicks are a powerful competitive edge.

WHY LISTEN TO US

We're ex-NSA hackers who know a thing or two about crushing fraudsters.

We help teams within corporations, affiliate networks, and media buyers assure that their environments are kept **proactively** safe from fraud. Our team of ex-NSA developers act as an extension of yours to eradicate the threat of fraud from your environment.

We understand that as affiliate marketers and media buyers, you get crushed by the bots and fake traffic on the web-it eats a gaping hole in your bottom line results. We've spent over a decade in affiliate marketing and this solution is handmade to solve the fraud issues in the ad industry.

That's why we're passionate about providing our customers with the most advanced measures possible in our proactive approach to preventing fraud...and we make it as easy as humanly possible for you and your team to implement and use.

Put this guide to use right away and contact us if we can help. You can email us at Justin@IPQS.com

Step 1: Don’t Pay Per Impression

A very common method of tracking digital advertising, is through CPI or Cost Per Impression.

However, **this can be dangerous** when you take into account that a big portion of those impressions, aren’t even human.

For example, if you are paying $0.0050 per impression, and your client's marketing budget allows for $100,000, they expect that you’ll get 20 million impressions. With just 20% fake traffic, however, this will actually result in only 16 million **human** impressions.

So... you are actually paying $0.00625 per *human* impression–this creates a big, problematic disconnect between expectation and results, which is bad for you and your client.

Instead, if you change your measure to charge for action (CPA), instead of impressions, you’ll have a much better chance of actually receiving the results that you paid for, not the ones fraudsters want you to see.

Step 2: Block Countries with High Rates of Bot Traffic

What’s one of the top ways to prevent bot traffic from accessing your advertising campaigns?

Block them at the source! Typically, fraudsters will reroute their bots and poor traffic through other countries using a VPN, where they are less likely to be detected by authorities (that was us at the NSA).

According to Ad Week, the rate of low quality and fraudulent traffic from countries such as China, Venezuela, Ukraine, and Singapore can be up to 92%!

For reference, the rate of poor quality traffic in the US is much lower at 43%. But still, **43% fake traffic?!**

You don't have to completely block these countries from accessing your sites, but at least block low quality sources from accessing your advertisers' campaigns.

You can do this by simply excluding where you don’t want traffic to come from, and focus on targeted areas with high quality traffic instead.

Step 3: Filter Traffic in Real Time

In order to successfully monitor your campaigns and ensure the best results for your advertisers, it's crucial to monitor and *filter* your traffic in real time.

The main benefit from using real time filtering, is that **fraudulent clicks won't touch your budget and won't lower your CPC rates**.

When analyzing your campaign while it's running, there's a few key metrics to keep your eye out for.

1. **Source of Traffic**
2. **Engagement with the Ad**
3. **CPC/CPA**

As described earlier, the source of your traffic can tell you a lot while assessing for poor quality traffic. By focusing on traffic from high quality locations, and excluding those with high rates of suspicious traffic, you'll immediately be doing yourself, and your advertisers, a huge favor.

Another key metric to track when looking for bots and fraudulent traffic is how they're actually *engaging* with your ad. Low engagement and high bounce rates are red flags for bot traffic.

Your Cost Per Click and Cost Per Action is usually related to the two points above.

Step 4: Fraud Prevention Softwares

While there are dozens of strategies to help prevent and minimize fraud risk, several of which were mentioned above, **there is only one sure fire way to detect and block fraud attacks** in real time.

This is through the use of an **anti-fraud prevention software.**

With tools that track and flag fraudulent IP addresses and allow you to assess and filter traffic in real time, you'll be saying goodbye to fraud on your media buys for good.

The only fraud prevention software that really works for you has these characteristics:

- **It prevents fake traffic automatically**
- **It uses Machine Learning and assigns a score to decide what to block**
- **It searches Blacklists of known fraudulent IPs**
- **It uses Honeypots to trap hackers and pull them away from your sites**
- **It employs Forensic Analysis* to determine fraudulent IPs that get past normal detection services**

***This is what our team used when we worked for the NSA to catch hackers for the US Government.**

What to Look for in a Fraud Prevention Software

You probably don't know much about Fraud Prevention Software–yet. We've created this guide to educate you about how they work and what you should look for to protect yourself.

If you're looking for an all-in-one fraud prevention solution that will increase peace of mind for both you and your advertising clients, then here's what you need to consider:

1. Timing

We mentioned this earlier, but it only makes sense that your Fraud Prevention Software is 100% proactive and **actually blocks fake traffic.** Otherwise, you're just paying someone to tell you how much money you've lost and there's nothing you can do about it.

Just so you know, IPQS proactively blocks fake traffic. You'll find out if you're seeing fraud on the 1st click, not the 10,000th after you've invested time and paid for traffic. Then, our API will tie into whatever platform you're using to block the traffic before the click is counted.

2. Pay Per Use Model

Without the right pricing model, fake traffic and even fraud could becomes a cost of doing business. It doesn't make sense to pay a company more to stop fraud than the fraud itself costs.

That's why we use a pay-per-use model. You only pay for the traffic we protect–nothing more. The best part is the first 5,000 clicks are on us, totally free for you so you can see an **ROI right away.**

3. Detects ALL Types of Fraudulent Traffic

Fraudsters have a number of tools for scamming you, so your prevention software should detect not only Proxies, but also Virtual Private Networks, The Onion Router (Tor), and any other type of IP spoofing software that fraudsters utilize.

Once an IP has been flagged, it should also be added to a blacklist to make sure it's always caught by others. IPQS does this automatically, and it constantly updates and checks IPs against our blacklist in real time.

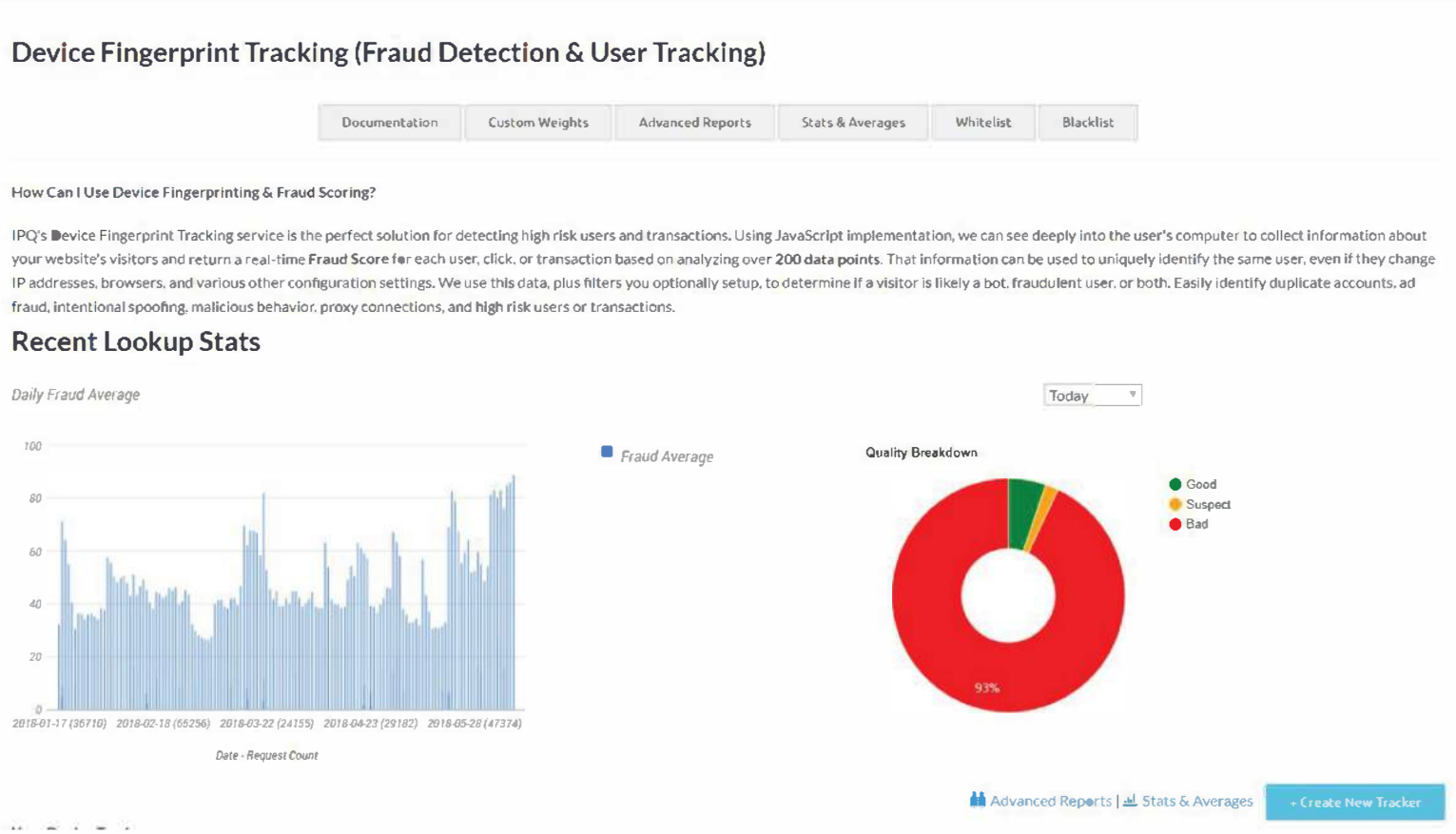
What to Look for in a Fraud Prevention Software (continued)

4. Device Fingerprinting

To catch ALL the ways fraudsters can take advantage, every IP should be "fingerprinted" in real time. This means gathering 200+ identifying data points from each individual user on the spot to create a unique device fingerprint. This data gives each user a fraud score that indicates the likeliness of the user to engage in fraud, in addition to other data such as a tracking ID, confidence score, location, and the status as a proxy or VPN connection.

IPQS is the only service capable of this.

By the way, **ecommerce fraud rates spiked 33% in 2016**, and as fraudsters get more and more sophisticated, it's harder and harder to tell what the real numbers are. Make sure you get a sophisticated team on your side, like the former NSA hackers we employ at IPQualityScore.



Fraud Prevention Glossary

In the spirit of helping quickly educate you on the important points of fraud prevention, here is a glossary of some of the terms we've used that you need to understand to know how fraud happens and how it is prevented.

Affiliate Fraud - Refers to any false or unscrupulous activity conducted to generate commissions from an affiliate marketing program. Usually involves fake/fraudulent clicks generated by bots and proxies, stolen credit cards that result in chargebacks, etc.

AVS - Address Verification System

Bot - A software application that runs automated tasks (scripts) over the Internet. Typically, bots perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone.

BotNet- A network of computers infected by a virus, usually controlled to do various tasks or attacks (DDoS).

Click Fraud - The practice of repeatedly clicking on an advertisement hosted on a website with the intention of generating revenue for the host site or draining revenue from the advertiser.

Credit Card Fraud – This type of fraud is committed when a stolen credit card is used to process a payment or when the customer intentionally disputes a payment for a legitimate product or service.

Dark Web - The portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser. People who access and utilize the Dark Web want to browse anonymously. There are a lot of legitimate people on it, but also a lot of bad.

Device Fingerprinting - IPQS tool that tracks over 250 data points to give a real time fraud score to users visiting websites. Excellent at detecting bots and high risk users.

Device ID - Unique super tracking ID that is assigned to a user by IPQS' Device Fingerprinting tool. Track users as they switch devices, browsers, etc. No one escapes our fraud detection!

Fraudster – A person who commits fraud with the intention of generating commissions and profits from invalid conversions.

Honeypot – A decoy computer system for trapping hackers or tracking unconventional or new hacking methods. Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.

Fraud Prevention Glossary (continued)

IP Address -Internet Protocol Address

Phishing – Phishing is a fraudulent attempt to acquire sensitive information. This is usually done through email in which the fraudster sends out a legitimate-looking email in an attempt to gather personal and financial information from recipients such as credit card number, social security number, account number or password. Phishing emails usually appear to come from a well-known and trusted sender.

Proactive Detection/Filtering - Performed in real time (usually on the click), IPQS returns a Fraud Score and Device ID in real time.The Fraud Score is based on scale of 0–100. Typical scores fall into these categories: 0–50 good, 51 – 75 suspicious, 75+ risky, 85+ high confidence of fraudulent behavior. This feature is the most effective method at preventing fake & fraudulent conversions so our service will keep your advertisers and partners happy,which will keep you happy.

Proxy - a proxy server is another computer which serves as a hub through which internet requests are processed. These are often used to mask the identity of the user, for example, a user in Russia can appear to be on a residential connection in the US.

Residential Proxies - These connections are very hard to detect and look like a normal IP address you would see on your home computer–but they can be part of botnets or some type of malware that allows users to tunnel into them and engage in fraudulent behavior. Most services cannot detect these, but naturally, PQS can.

Spoofing – Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

Tor (anonymity network) – Free software for enabling anonymous communication. The name is an acronym derived from the original software project name The Onion Router. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

VPN - Virtual Private Network (usually done outside of a browser as a standalone application) - using a data center IP address or something obvious.