trafficguard

Ad fraud prevention

Buyer's guide for ad networks

Contents

A buyer’s guide for ad networks

As advertisers demand greater transparency from their supply partners with regards to ad fraud, there is an opportunity for ad networks to create strong competitive advantages by removing invalid traffic*.

From time consuming invoice reconciliations to restricted client campaign optimisation and potential reputational damage, the impacts of fraud are significant and ultimately reduce your revenue and growth potential.

* **Invalid traffic (IVT)** is when interactions with advertising are not from legitimate consumers. In cases where IVT is intentionally created to attract ad spend, it’s considered ad fraud.

Fraudsters are becoming increasingly sophisticated in their efforts to evade detection and trick attribution platforms. As a result, there are a large number of solutions to help you defend your business from ad fraud. Fraud prevention is not a tick box exercise but a spectrum, with different solutions offering varying degrees of protection.

There are three steps in the process of evaluating different fraud prevention solutions and where they sit on the protection spectrum:

Step One

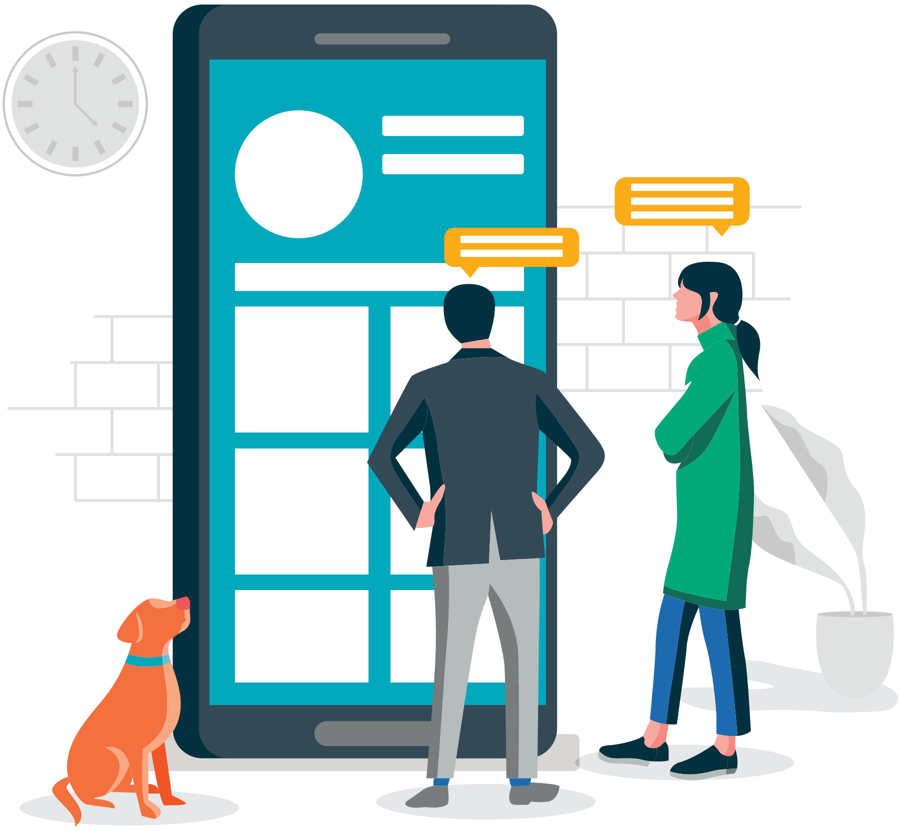
Understanding all the ways that fraud impacts ad networks

Step Two

Identifying the capabilities required to address these costs

Step Three

Evaluating alternatives based on their capabilities



Step One:
Costs & Impacts of ad fraud

Juniper Research estimates that by 2023, the global cost of digital advertising fraud will reach US$100 billion.

Aside from wasted media spend, there are many other indirect costs which can impact revenue and growth potential of ad networks. The extent of these costs varies depending on the level of fraud protection you employ. Understanding the total cost of ad fraud will help you select a fraud protection partner that addresses the specific challenges of your business.

[1] 2019, Juniper Research, Press Release (https://www.juniperresearch.com/press/press-releases/advertising-fraud-losses-to-reach-42-bn-2019)

1. Time wasted on media volume reconciliations

Ad networks typically spend considerable time negotiating the volumes of valid traffic and conversion volumes with clients and with supply partners.

In their attempt to claw back ad spend, some advertisers even try to strong-arm networks into reducing billed traffic volumes by claiming (sometimes with little or no proof) that traffic supplied is low quality or fraudulent. Because networks want to keep their clients, they usually end up giving in - leaving the networks to recover costs with their partners or else be out of pocket.

Invoice reconciliation is time consuming, error prone and a costly exercise for all parties involved. Time spent in this activity is also an opportunity cost as it takes your team away from tasks that could deliver superior campaign performance.

To mitigate this cost, read more about these capabilities in Step Two:

- Prevention capabilities
- Transparency and granularity of reporting
- Accuracy and reliability of fraud detection

2. Out of pocket costs after chargebacks and refunds

Refunds paid to clients after media volume reconciliations can leave you open to the risk of being out-of-pocket due to the shorter payment terms ad networks usually pay partners on. Typically, ad networks have already paid supply sources when volume disputes with advertisers arise. This leaves you having to claim credits from your suppliers, in an effort to not to be left out-of-pocket.

To mitigate this cost, read more about these capabilities in Step Two:

- Prevention capabilities
- Transparency and granularity of reporting

3. Performance impacts on client campaigns

After a client campaign commences, you will begin to optimise and then scale activity with the best performing sources. When you don't have visibility of which traffic is fraud and which is valid until the end of the month when an advertiser shares their report, optimisation is virtually impossible and scaling is blind. Without a real-time understanding of valid and invalid traffic, there is a very real risk that you are scaling with sources that are delivering a high proportion of fraud. Sometimes clients may even ask you to scale with fraud inflated sources before checking their quality reports, only to then request substantial quality-based refunds at billing time.

Not only does this compound invoice reconciliation at billing time, but it means your campaign allocation is underutilised.

When you have access to clean data, optimisation is essentially real time because you don't inadvertently scale with sources inflated by fraud. If you lack confidence in the data or simply don't have access, optimisation carries an element of risk and may restrict the performance of the campaign.

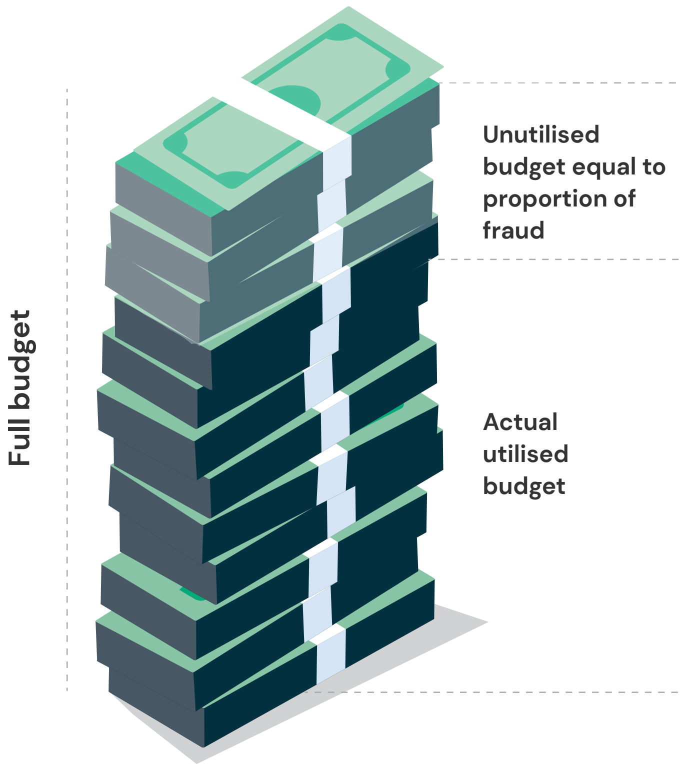
To mitigate this cost, read more about these capabilities in Step Two:

- Coverage level
- Stage in the journey
- Transparency and granularity of reporting

4. Underutilised budgets and campaign caps

In a sea of ad networks competing for client ad spend, it is becoming increasingly difficult to differentiate from your competitors and earn your share of the market. With the transient nature of advertisers frequently switching ad networks, you may struggle to retain clients if budgets are being underutilised. The proportion of invalid traffic present in your campaign is the minimum client budget that you're leaving on the table.

For example, if 25% of conversions delivered to a client are fraudulent, 25% of the budget will be refunded to the client at the end of the campaign. This means that only 75% of the budget has been utilised to deliver conversions. Underutilised budgets, not to mention eroded trust, may encourage the advertiser to look for new networks.



On the flip-side, removing fraud in real-time and utilising 100% of budgets on valid traffic increases the likelihood of clients renewing their budgets. If the campaign delivers strong conversions and utilises the budget before the end of the period, the advertiser may even choose to increase their budget with you. This opportunity to grow revenue with clients is lost if there is fraud consuming ad spend and diminishing optimisation opportunities.

To mitigate this cost, read more about these capabilities in Step Two:

- Prevention capabilities
- Channel coverage
- Stage in the journey
- Independence

5. Damaged reputations and loss of trust

Over time, the presence of fraud in the traffic supplied to clients is certain to start eroding trust. Once damaged, it can be difficult for you to rebuild that lost trust with clients. As a result, it isn't uncommon to see advertisers frequently changing their networks and supply partners; making it even harder for you to build trust with clients.

To mitigate this cost, read more about these capabilities in Step Two:

- Prevention capabilities
- Machine learning
- Transparency and granularity of reporting

6. Threat of litigation

Unresolved conversion volume disputes with advertisers can expose you to costly and time consuming legal disputes. The recent Uber vs Fetch case has set a precedent for advertisers taking legal action against intermediaries for unresolved fraud claims. As the media and advertising industry continues to discuss ad fraud, it is likely we will see more examples of this kind of case. The balance of power is with the clients and therefore the risk of litigation is significant when disputes on valid traffic volumes arise – especially when there is no independent ad verification in play.

To mitigate this cost, read more about these capabilities in Step Two:

- Machine learning
- Transparency and granularity of reporting
- Coverage level
- Independence

7. Perpetuating fraud

Relying on refunds and chargebacks as a solution to ad fraud means that somewhere in the chain, an intermediary is swallowing the cost of fraud. This doesn't solve the problem, but perpetuates it. Fraudsters are still being paid and are encouraged to continue evolving their operation to evade detection.

To mitigate this cost, read more about these capabilities in Step Two:

- Machine learning
- Prevention capabilities

Step Two:
Identifying fraud prevention capabilities

Fraud prevention is far from a tick box exercise. If the solution you select does not provide adequate protection, you may be lulled into a false sense of security – thinking you are protected from fraud, but campaigns are actually still vulnerable. Or worse, your fraud protection solution maybe mistakenly blocking valid traffic, impacting the results you can deliver for clients and your earning potential.

These are the most important factors and capabilities to look for when evaluating fraud prevention solutions.

Prevention capabilities (not just reporting or scoring)

Some solutions only detect invalid traffic, leaving you to interpret reports and determine an appropriate course of action to minimise the impact. This reactive approach means that fraudsters keep getting paid and optimisation is severely compromised.

On the other hand, solutions that reliably remove* invalid traffic use their specialist knowledge to identify and remove fraud from your campaigns. Prevention is a proactive approach that allows you to leave fraud mitigation to the specialists and focus on optimising your campaigns and growing your business.

* **When we refer to removing fraud,** it means that invalid clicks are filtered out. Installs that are deemed invalid still occur, but the attribution of them is blocked so that you don't pay for them.

How to tell if a fraud prevention tool isn't surgically removing fraud:

Provision of risk scores and reports of 'suspicious' traffic rather than blocked or removed traffic reports

Detection of fraud only, no blocking

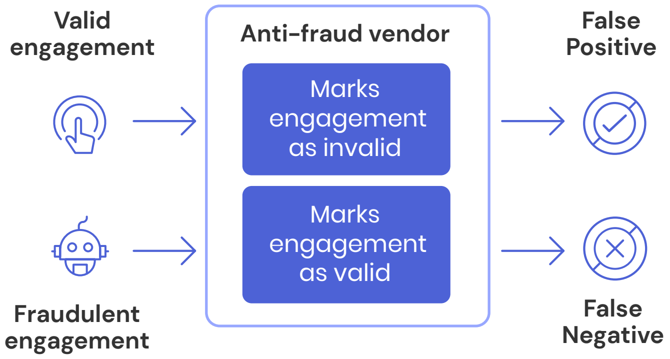
Accuracy and reliability of fraud detection

When reviewing anti-fraud vendors, be careful not to fall into the trap of thinking that Vendor A is better than Vendor B because Vendor A blocked more fraud than Vendor B. Volume of traffic blocked is not a reliable indicator of effectiveness and may actually show that Vendor A is blocking valid traffic, thereby reducing your earning potential.

Rudimentary detection relies on blacklists or basic rules engines. Sophisticated fraud prevention adds to this with behavioural analysis, relational graphs and machine learning to analyse combinations of indicators over time and across devices in order to reliably mitigate fraud and reduce the risk of false positives*.

Traditional anti-fraud tools provide risk scores to transactions rather than categorising them as invalid. On the other hand, tools developed by data scientists that specialise in fraud prevention are more transparent with what is invalid and why. Looking for solutions that are transparent with fraud reasons and definitions on a granular transaction level is a good sign that they are happy to stand behind the science in their fraud detection.

Flow of false identification



* **False positives** occur when a valid install is marked as fraud. False negatives are when solutions fail to catch fraud, marking it as valid.

How to tell if a fraud prevention tool is relying on rudimentary detection:

- Reliance on blacklists or basic rules engines
- No evidence of machine learning
- Provision of risk scores, no actual blocking

Transparency and granularity of reporting

Granularity of data provided in reporting varies significantly between anti-fraud vendors. Some vendors operate a "black box" where they refuse to share details of why traffic has been invalidated. If you don't know why traffic has been invalidated, how will you trust that the black box isn't blocking your valid traffic?

To have confidence in the data and the reasons for fraud being blocked, you need access to granular detail explaining the science in the diagnosis for every transaction. This confidence and access to real-time reporting will help you save time, reduce chargebacks and deliver strong ROAS for clients.

How to tell if a fraud prevention tool is a 'black box' vendor:

No invalidation reasons provided

Invalidation reasons vague

Invalidation reason not available on a transaction basis

Stage in the journey

Many solutions focus solely on one stage of the journey (ie. click) and do not provide analysis or fraud mitigation across impression, install or event levels. Solutions that can see click level data can use this data to start blocking fraud at the click. Likewise, solutions with visibility of the install can mitigate IVT at the install. Solutions that can block at both not only mitigate fraud based on click and install level data, but also the data that comes from comparing the two levels for discrepancies. As fraud becomes increasingly sophisticated, this level of visibility is essential and helps to mitigate fraud sophisticated enough to evade earlier levels of detection.

How to tell if a fraud prevention tool provides single-level coverage:

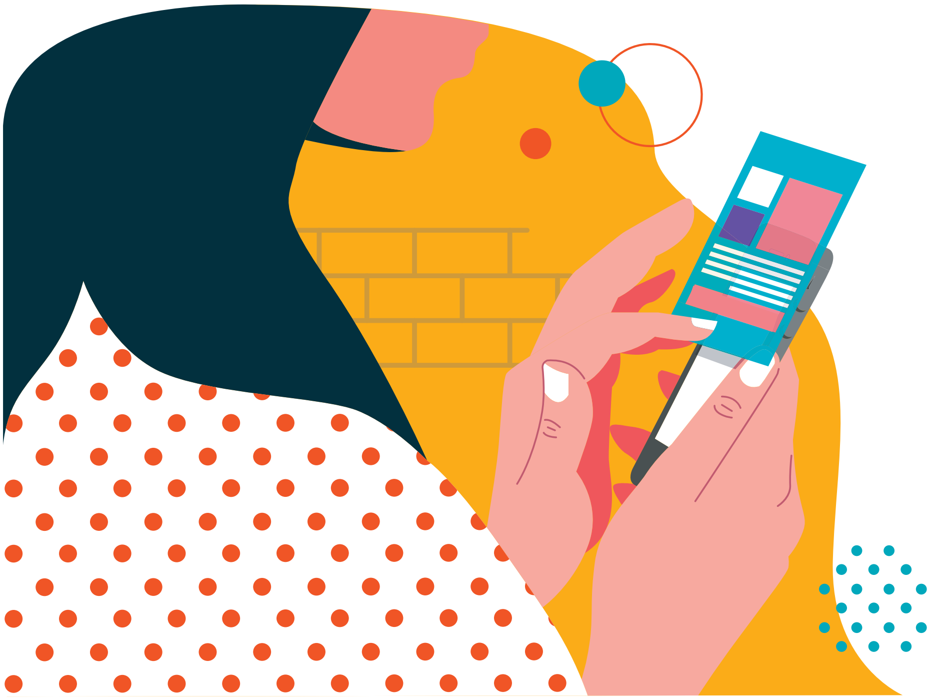
Reporting of only removed / detected impressions, clicks or install atrributions

Machine learning

Ad fraud is constantly mutating and becoming more sophisticated to avoid detection. Anti-fraud tools have varying capabilities to detect and block unknown types of ad fraud as they emerge. Tools relying on rules engines or IP lists cannot detect fraud they have not seen before, leaving you exposed as fraud evolves. Companies that utilise a combination of rules engines and machine learning algorithms which learn from the continuous data loops will provide far greater protection against both known and unknown fraud tactics.

It is also worth noting here that many companies claim to be utilising machine learning in their ad fraud prevention tools. In order to separate true machine learning capabilities from marketing spin, look for:

- Evidence of a data science and analytics team
- Evidence of systems and infrastructure necessary to run machine learning and process big data
- Ask questions about the specific machine learning algorithms utilised by the tool. If the answer is incomplete or there is no legitimate answer, you can make assumptions about the true capabilities of the tool.



How to tell if a fraud prevention tool doesn't have true machine learning capabilities:

- No evidence of data science or analytics team
- No evidence of tools or infrastructure to run ML and process big data
- Cannot answer questions around specific ML algorithms used

Independence

Utilising a third party vendor to identify and remove fraud gives you a verified, unbiased view of the quality of the traffic you send to your clients. This gives you the confidence and the evidence to address any volume discrepancies between your network and the advertiser.

There are a number of potential conflicts of interest that an anti-fraud solution could have.

- Pricing conflict - When pricing is tied to volumes of IVT detected, vendors are incentivised to report higher volumes of fraud so that they get paid more. This has the potential to result in false positives, reducing your earning potential and skewing your data. When pricing is tied to valid traffic processed, the opposite is true.
- Service conflict - The key objective of campaign management platforms (CMPs) and mobile measurement platforms (MMPs) is to measure and attribute valid traffic to the correct sources. These are the very functions that fraudsters try to exploit in order to make money. Because of this, these services should be doing their utmost to correctly attribute in the first instance, rather than upselling a fraud prevention solution.
- Competitive conflict - Recently we have seen the rise of anti-fraud tools being offered to networks and brands by other ad networks, ie your competitors. Utilising these solutions helps your competitors grow their position, their revenue and their data assets at your expense.

For unbiased and conflict free identification and removal of invalid traffic, your fraud protection partner should be an independent service and you should be charged based on the number of transactions processed, not the volume of fraud detected.

How to tell if there might be a conflict of interest:

Pricing model is tied to volume of fraud detected

Platform responsible for attribution is also providing fraud protection - like marking your own homework

Platform responsible for fraud prevention is or owns an ad network

Integration methods

How an anti-fraud tool integrates dictates its compatibility with different types of networks. For example, solutions that rely on custom API integrations* require significant infrastructure on the client side, making it difficult for networks with smaller budgets to integrate. Solutions with a greater variety of integration methods provide greater flexibility and are able to offer services to different types and sizes of clients.

* **An API (application programming interface)** is a software intermediary that allows two platforms to communicate with each other.

The following table provides an overview of the most common integration methods utilised between ad networks and anti-fraud vendors and the implications of each.

Integration Method	Description	Implications
Measurement URL	Data is passed to anti-fraud solution via a tracking URL.	Anti-fraud solution is able to block fraud in real-time. There are no complex integrations making it easy to access for budgets of any size.
API	Customised integration through proprietary platform.	Requires significant development work to integrate, so is only really accessible to networks with large budgets. Unable to block at click level in real-time, but can block before attribution (depending on the capability of the campaign management platform/s).
Platform integrations	Integration through campaign management platform such as HasOffers, Partnerize etc.	Simplest integration method if network is using the third party campaign management platform. Ability to block fraud depends on the vendor's integration with the platform.

Coverage level

Some fraud protection solutions are only built to process samples of transactions as opposed to every transaction. Sample testing may not wholly represent the risk and increases the chance of false positives/negatives, reducing supply volumes and earning potential.

Selecting a tool that analyses every transaction to detect and remove fraud surgically will enable you to deliver strong results for your clients and reduce the risk of litigation due to incorrect or missing fraud diagnoses.

How to tell if a fraud prevention tool relies on sampling:

Transactional level detail is not available in reporting

Channel coverage

Some tools have a single focus on one channel ie. mobile or desktop. Advertising is largely moving to a more personalised, cross-device model in order to appeal to customers however they are accessing the internet. Omni-channel coverage allows anti-fraud solutions to gain an understanding of 'normal' user behaviour and usage patterns, which enables them to quickly identify any behaviour outside of the norm likely to be fraudulent.

How to tell if a fraud prevention tool provides single-level cover only:

Analysing traffic at one point only - such as impression

Utilises JS tags only or anti-fraud solution provided through MMP integration

Step Three: Evaluation

By understanding the capabilities of a fraud prevention solution and identifying potential weak spots, you arm yourself with the knowledge to select the best tool to address your most pressing challenges. The following table summarises the various capabilities and gives you some key questions to ask if you are unsure about whether the solution you are reviewing will address the specific challenges faced by your network.

Capability	Description	Questions to ask
Blocking vs reporting	Ability of a fraud protection solution to block fraud in real-time, or detect / provide risk scores only.	• Do you identify invalid traffic or provide a risk score? • Can you block/filter/remove invalid traffic before a supply source is attributed?
Reporting	Provision of granular reporting detailing IVT blocking reasons; in real-time to all parties in the supply chain.	• Can you give me the reasons for every transaction marked as fraud? • Can I see reporting by site ID?
Stage in the journey	Stage in the advertising journey when fraud detection or blocking occurs – impression, click, install or event.	• Which stage in the advertising journey do you detect fraud? • Do you analyse multiple stages including the impression, click and event levels looking for indicators of fraud? • Do you block fraud at these stages?
Machine learning	Utilisation of sophisticated machine learning algorithms to detect new fraud tactics as they emerge.	• Can you explain the ML algorithms and models used to identify fraudulent transactions? • How big is your data science team? • Is there any other demonstration of their data science capability either in research papers, tech case studies, thought leadership content?
Pricing model	How the vendor charges you for their services, ie. fixed price, price based on volumes of IVT detected, transaction based pricing.	• What is the reasoning behind the pricing model of the solution? • How do you prevent misattribution of conversions?
Integration methods	The way you can integrate with the ad fraud protection tool, ie. API, SDK, URL redirect.	• How do we integrate with your tool? • Do you have an integration with my MMP?
Coverage level	Whether the tool relies on blacklists or sampling; or surgically removes fraud through analysis of combinations of indicators over time.	• What methods do you use to identify fraud? • Do you analyse every transaction, or utilise sampling?
Channel coverage	Coverage across advertising channels – ie. mobile, desktop, mobile app.	• Do you provide coverage across multiple advertising channels, including mobile, desktop and mobile app?

In Summary

Fraud prevention is a spectrum, not a tick box exercise. Different solutions offer varying degrees of protection from the many impacts and costs of fraud to any ad network.

Time consuming invoice reconciliations, difficulty building trust with transient advertisers and reckless blocking of entire traffic sources are just some of the costs of fraud that might be impacting your network's success. Understanding and addressing all of the costs outlined in this guide empowers you to save media spend and protect your future growth and revenue potential.

There are a number of solutions that claim to address invalid traffic but may still be leaving you vulnerable to fraud. Asking questions around machine learning capabilities, pricing models and coverage level can help you decide whether the tool you are reviewing will provide you with the strongest defence against ad fraud.

The way forward is the full utilisation of multipoint fraud mitigation tools that detect and block invalid traffic surgically, in real time. This will help you fully utilise client budgets, encourage trust and transparency with all partners and clients and help you differentiate your business from other ad networks.

About TrafficGuard

TrafficGuard provides comprehensive ad fraud protection for brands, apps, agencies and ad networks. Purpose-built specifically to fight ad fraud, TrafficGuard analyses multiple stages in the advertising journey - impressions, clicks and events such as sales or app installs - to remove invalid traffic at the earliest reliable diagnosis. By doing this, TrafficGuard improves campaign optimisation, drives ROAS and saves time usually wasted on media volume reconciliations.

For ad networks, TrafficGuard's surgical approach to fraud mitigation is particularly appealing as it removes invalid traffic whilst also protecting valid traffic from false positives.

trafficguard

Knowledge is power! Get the full picture of the sources supplying invalid or low quality traffic with a free, no-obligation Traffic Quality Audit.

BOOK AUDIT