NS8

Beginner's Guide to Ad Fraud

An eCommerce merchants guide

Contents

Introduction

Advertising fraud is a common problem. Unfortunately, no one really knows how common this problem really is or the impact it has had on digital advertisers. Estimates for the amount that ad fraud has stolen vary by billions of dollars, and studies on the effects of malicious bot traffic (known as IVT) often conflict.

One of the main reasons for the discrepancies is the opaque nature of the digital advertising industry. Most of the time, analytics on advertising come from the companies that sell advertising. Adding to the frustration, there are few regulations in place to protect advertisers. The regulations that do exist are difficult to enforce because ad fraud often crosses borders and jurisdiction is difficult to establish.

That leaves individual companies to fend for themselves. With so little solid information available, many companies simply rely on the ad agencies and networks they work with to police themselves. However, there's very little incentive for the ad industry to change because they make money whether the views are real or fake.

So what can you do about ad fraud? Well, the first step to fighting ad fraud is to understand what it is and how it works.

Common Ad Fraud Schemes

Ad fraud is complicated because there are a variety of ways that money can be diverted from advertising budgets. Many of these scams take very little time to set up, and they can be very lucrative. Some of them often overlap and are used together. These are just a few of the most common ad fraud schemes. Note that they change often and adapt to new technology quickly.

RETARGETING FRAUD

Retargeting advertising is one of the most powerful tools for an online business. The ability to target high-value potential customers and users who have already shown interest in your products or services has been a revolution for the online advertising industry.

You as a consumer may have even noticed retargeting in action. Have you ever seen ads for a product you were researching, or almost purchased, following you around the internet for several weeks? That is what it is like to be remarketed to.

So how do the scammers profit from retargeting fraud? Retargeting fraud is ultimately a simple scam. Bots are sent to a business's website in order to get tagged for retargeting ads. The bots are then sent to the fraudster's website to "look" at the ads that the business is paying to display.

This is how it works:

1. Your business buys some ads from an ad network.
2. Meanwhile the fraudster rents some bot traffic. The traffic is dirt cheap and can be had for a fraction of a cent per action.
3. The bots are disguised as normal users. Then the bots are sent out to search engines and social networks to find active advertising campaigns.
4. The bot traffic uses high-value search terms to find websites like yours that are actively spending advertising dollars for paid search results.
5. The bots pretend to shop. They are programmed to interact with the business's website like normal users would. They perform specific actions that the ad network is watching for, called success metrics. In many cases, the success metric is placing items into a shopping cart.
6. Ad networks use these success metrics to determine which audiences a user should belong to. Due to this, the ad network unknowingly tags these bots as high-value users and places them into audiences to potentially be shown retargeting ads.
7. The bots then abandon their shopping carts. The ad network witnesses another success metric, cart abandonment, and records the behavior. The bot is now placed into the campaign audience to be served ads for items they "almost" bought.
8. The business executes its monthly advertising buy, including retargeting ads. (Note: The business has not made a mistake and is simply following the best practices.)
9. The bot traffic is directed to the fraudster's websites. This is where the fraudster

gets paid. Bots register views and click on the high-paying retargeting ads being displayed on the fraudster's websites.

10. The fraudster repeats this thousands of times. The scale and speed at which advertising fraud and retargeting fraud can be executed is staggering. For the fraudsters it is a simple equation, they get more for every click than it costs them. It's free money.

11. The ad network continues to display ads until the ad spend is exhausted, which is when the bots move onto the next business with a fresh budget or prepare to do the same thing again with a new product.

Because the bots are made to blend in with human traffic, estimates of how often this happens and how much money is lost to it vary significantly. Many companies have no way to tell at all whether or not retargeting fraud is affecting them.

CLICK FRAUD

Click fraud occurs when fake clicks are registered on an advertisement. Many ads are sold as Pay Per Click (PPC), which means that advertisers are charged for every "click" made on the ad - regardless of the user's actual interest. Whether clicks are made by genuine users, bots, or competitors, the advertiser still gets charged.

Click fraud is popular because it's relatively easy to do. In the past, real human traffic was often used to generate fraudulent clicks by employing hundreds of people in "click farms". These people were paid to sit and click on ads all day despite having no interest in the company or services. Then more subtle ad-clicking scams came about, presenting themselves as work from home jobs. Employees believed they were simply "reviewing ads" and often had no idea that they were being used to perpetuate advertising fraud.

More recently, due to the lower costs and advances in automation, using bots to click on ads has become the preferred method for many fraudsters. By using software that is designed to mimic real user behavior, fraudsters can rapidly generate thousands of fake clicks on a given ad. Even if most of the bots are identified as invalid traffic, the ad networks will register some as high-quality real human users and charge advertisers to display future ads to them. With so many bots, fraudsters can make a lot of money quickly with little effort.

This is how it works:

1. Thousands of bots are scripted to click on an ad for organic supplements that is being displayed on another website.
2. The bots keep clicking and many are now registered as high quality "health and wellness" users, which are considered very valuable by the ad network.
3. The fraudster then directs this traffic to their own website, and the ad network displays similar ads to them that match the "health and wellness" audience tag they have been given.
4. The bots "view" or "click" on these ads and the fraudster gets paid.
5. The loop continues until the ad network discovers the scheme and stops sending ads or tags the website as fraud. When this happens, the fraudster simply creates a new site and begins all over again.

As with retargeting fraud, it is incredibly difficult to understand exactly how much money click fraud is draining from the digital advertising industry. Some ad networks have tried to crack down on click fraud and do find some schemes.

SPOOFING

This type of ad fraud incorporates several methods. In general, spoofing refers to selling advertisers something different than what they are getting. Common examples include user agent spoofing, SDK spoofing, and domain spoofing.

Spoofing is often used in conjunction with other forms of ad fraud. Schemes can be incredibly complicated or very simple, but they are often effective due to a lack of tools available to root out this type of fraud.

Here are a few ways it can work:

1. A publisher codes several bots to view ads on their site. The bots are given data, called user agent strings, that identify themselves. These user agent strings are made to appear as different browser and device combinations to look like real visitors. A single bot may even run through several user agent strings to appear as several different visitors, driving up the ad views and costing the advertiser more money. This is user agent spoofing.

2. A fraudster develops a simple free app. When the app is downloaded, it puts a cookie on all the devices. They get hired as an affiliate to push downloads of an advertisers app. When the fraudster activates the code left on the devices, they register a download for the advertisers app even though the person with the device never actually downloaded the second app. The advertiser pays out the fraudster for commissions believing all the downloads were real. This is SDK spoofing.

3. A site that has adult or controversial content is not selling enough ad spend. The create a url that is similar to a well-known and trusted publisher and redirect it to their site. They then sell the url and masquerade it as the trusted publisher for a lower cost. Advertisers purchase what they think is the trusted publisher but end up advertising on sites that are not brand safe. In programmatic advertising, this

is made even easier as some allow publishers to declare their own domains and site IDs. This is known as domain spoofing.

Spoofing can be particularly damaging for companies because they may lose more than just money. With SDK spoofing, companies think they have more customers and a higher base. If they then sell their own ads based on this information, they could be committing fraud themselves. For domain spoofing, companies could lose future customers for advertising on websites that publish content not appropriate for their audience.

CASH-OUT SITES

Advertising is an essential part of running an online business. Increasing demand from ad buyers has led to a need for high quality advertising space that can generate new leads. However, the digital advertising process is complicated with little transparency. Often, this can mean that advertisers pay for ads on sites that no human actually sees.

These sites, known as "cash out" sites, are built specifically to run ads. Essentially, a fraudster will set up a fake site that is made only to serve ads to bots.

This is how it works:

1. A fake website is created and populated with things like celebrity gossip, news, or other popular content.
2. Cheap bot traffic is purchased and routed to the new website. This makes it seem as if the website has a lot

of online visitors browsing through their content.
3. Ad networks see that this site is getting a lot of traffic and include it in their inventory for sale to ad buyers.
4. Advertisers buy ad space on the site, and the fraudster gets paid a lot of money in advertising revenue.

Most of these sites attract virtually no traffic other than bot visitors, which means that advertisers spend a lot of money on ads that are never viewed by real people. Over the years, this scheme has become so lucrative that some studies now indicate that 1 in 5 of all websites are "cash-out" sites.

AD STACKING

Slightly different from other forms of ad fraud we've discussed here, this form actually relies on real human customers viewing ads. Ads are hidden behind other ads, but they are loaded and "shown" to real customers. Unfortunately, only the top ad can be seen.
Ad stacking is able to persist because there is no standardized measure for a "view" on an ad. Many companies simply require that at least half the pixels for an ad be viewable for a half a second. This registers as an impression. Because webpages can take several seconds to fully load, customers often don't even notice if an ad frame flickers while loading. Those flickers, however, are sometimes multiple ads being loaded in the same frame.

This is how it works:

1. A publisher creates a site, including advertising space they will sell.

2. They then turn to ad exchanges, agencies, and direct sales to sell the advertising space on that site.
3. When a person comes to the site, the page loads and shows them ads in those spaces.
4. What the visitor can't see is that each ad space is actually loading several ads, stacked on top of each other. Only the top ad is visible once loaded. However, many ad exchanges and agencies register each ad as being viewable because they loaded correctly and met the minimum requirements of half the pixels being visible for half a second.
5. All advertisers are then charged by the publisher, even though most ads were never seen by a customer.

Ad stacking can be difficult to detect because the ads are loading correctly. Some ad networks have tools or will block sites with too much activity, but publishers can get around this by selling their space on multiple networks.

AFFILIATE FRAUD

Affiliates can be a great way to get exposure for a new brand. When done correctly, the system can benefit everyone. Many younger customers trust recommendations from people they follow on social media.

This is how it works:

1. An advertiser finds an affiliate and agrees to give them a commission for bringing people to their site. They get a bigger commission for people who make purchases.
2. The affiliate posts a tracking link and encourages

followers to go to the site.
3. They push friends/other affiliates to follow the link and make a purchase.
4. The company gets visitors and purchases that are linked to the affiliate and pays out their commission.
5. The friends/other affiliates that made purchases submit refund requests or chargebacks for the items purchased.
6. The company loses both the amount of the purchase as well as the money paid to the affiliate.
7. The affiliate then move on to the next company.

Some affiliates have even been found to use malware and cookies that attribute sales to their link even when they have nothing to do with the sale. It took Facebook several years to find one of these scams.

PIXEL STUFFING

This type of ad fraud was more common in the past but can still occur on ad networks with less controls in place. Similar to ad stacking, pixel stuffing is a way of putting many ads on a single page without the customers realizing it. It's a way to fit a lot of ads on a single page without affecting the customer experience.

Every screen is made up of thousands of pixels. More pixels on a screen means better resolution and a clearer picture. A single pixel is virtually impossible for the human eye to detect. Fraudsters use this to their advantage by creating ad frames that use only a few pixels or even just one.

This is how it works:

1. A publisher creates a website and attracts visitors.
2. They create advertising space with frames for the ads that are minuscule (one or just a few pixels in size).
3. The publisher lists their ad space with advertising networks, agencies, and direct sales.
4. Advertisers buy advertising space on the site.
5. When visitors arrive, ads are loaded into the small frames. The visitor cannot see the ads, but the advertiser is charged for the view.

Some ad networks and agencies have developed ways to recognized small size frames and will weed out these types of publishers. Others still have no detection methods for these types of ad frames. Because each network and agency has different controls, your exposure to these scams will vary.

AD HIJACKING/AD INJECTION/MALVERTISING

Different from everything else on this list, the goal of these types of ad fraud are not necessarily about making money. They are often done by competitors or other advertisers rather than fraudsters attempting to redirect your advertising budget into their own pockets. However, ad hijacking, ad injection, and malvertising can both cost you customers and significantly affect your bottom line.

This is how it works for hijacking:

1. You set up a Pay-Per-Click search ad for a branded keyword.
2. A competitor/reseller/affilieate also sets up a PPC search

ad for the same keyword, bidding just above you.

3. In the title and metadescription, the competitor uses the same or very similar titles and information to what your ad says, sometimes even using your display URL.
4. Their ad is displayed either above yours or instead of yours on the search results page.
5. When a customer clicks on the ad, they are redirected to your competitor or to your site with an affiliate cookie or reseller code.
6. Customers may end up purchasing from your competitor or, if they make a purchase on your site, appearing as if they came from an affiliate or reseller link. You then pay a commission or lose a customer.

This is how it works for injection/malvertising:

1. You have advertising space on your website.
2. That ad space is programmatically purchased by other advertisers.
3. Customers come to your site and while browsing receive intrusive ads that redirect their browsers or link to unsafe sites.
4. The customers get frustrated with the experience and stop using your site. Even worse, they may share their experience on social media or with friends and cause others to lose trust in your company.

With malvertising, ad networks often have no idea what is happening. Because of targeting tools, bad advertisers can use specific targeting tactics to only go after certain types of people. The complexity of the digital advertising system makes it difficult for the ad networks to find these specific targets. To them, the advertisements seem legitimate. You may not even know that these ads are being shown on your site.

Common Ad Fraud Solutions

There are a few different ways that advertisers can protect themselves from ad fraud. Some are more effective than others, and they can vary significantly in cost. Many of them are often paired together as well. Here are a few of the most common solutions in use today:

NOTHING

As previously stated, the most common solution companies employ against ad fraud is nothing at all. Even companies that understand ad fraud is a known problem often write it off as a necessary expense of utilizing digital advertising. But it doesn't have to be.

While no solution will completely eradicate ad fraud, doing nothing to prevent it is essentially throwing your money away. There's no reason to waste more money on something that you know is a problem. The key is to find the right balance of cost and effectiveness in your prevention strategy to maximize your ad dollars. There's little benefit to doing nothing to prevent ad fraud, and it could end up costing you far more than you realize.

SELF-REGULATION

Similarly, a lot of companies expect ad agencies and networks to self-regulate. Utilizing the tools available from your ad network, agencies, and other partners can be a great first step for reducing ad fraud. However,

the lack of transparency in digital advertising means that you are blindly trusting those companies to have your best interests at heart.

Using other methods to audit or verify their results can actually help strengthen your knowledge about those companies and how effective your campaigns are. Relying entirely on them to explain when and if fraud is occurring could cause you to spend money on the wrong campaigns, hurting your bottom line. However, asking for more transparency and tools can help push the industry in the right direction to curb fraud problems.

ADS.TXT

As a way to fight back against domain spoofing and unauthorized resale of ad space, the Interactive Advertising Bureau (IAB) Tech Lab came up with the ads.txt campaign. The campaign requires companies to attach a .txt file that lists authorized publishers to each advertisement. It's relatively simple for websites to implement and, more recently, has expanded to include apps as well. Because it doesn't cost anything and can be put in place by publishers themselves, IAB assumed it would be an easy and helpful step to help curb a specific type of fraud.

There are a few drawbacks. First, its strength relies on wide adoption of the system. Though there are more companies using it today than when it first launched, there are still a number of publishers that don't use ads.txt at all. That makes it less valuable because advertisers limit their reach if they only work with publishers that use it.

Second, the actual effectiveness is unknown. There have been a few studies showing that early adopters have seen less fraud, but there could be a variety of reasons for that correlation. Plus, many ads.txt files have been found to have errors, outdated information, or other issues. That renders the file less valuable and could even mean that ad networks simply don't use the file at all. Because individual publishers are responsible for keeping their files updated, it can be difficult for smaller companies to ensure their lists are up-to-date and research each company that asks to be included.

Finally, it only addresses a very specific form of ad fraud and seems to mostly target resellers. While this is a problematic part of the digital advertising industry, it does not address many of the larger problems that exist due to ad fraud. To be truly effective, it has to work in conjunction with a lot of other solutions.

BLOCKCHAIN

Sometimes hailed as the total solution to ad fraud, blockchain is meant to make the very opaque system of digital advertising more transparent. Blockchain is simply a process of recording every step that occurs in a transaction. For digital advertising, this would follow from the moment an ad is purchased until it gets displayed, played, or clicked.

Because each step would be accessible on a locked public record, every advertiser would be able to recognize when a problem occurs between their purchase and the end result.

While this would be great for accountability and transparency, it doesn't address many of the issues that occur with ad fraud.

There is no prevention in place using blockchain. Although you could more easily recognize that fraud has occurred, there's no way to stop it from happening in this system. Additionally, everyone from the advertiser to the final publisher has to use the same blockchain process. There are currently several in use. Added to all of this, programmatic bidding happens in fractions of a second. Blockchain, at this time, is a slower process. In the end, blockchain may be a great way to handle direct publisher ad buys to audit for any fraud, but it is not a complete solution for now.

TRAFFIC/CAMPAIGN SCORING

A common method of fraud prevention, traffic/campaign scoring can be fully automated or more manual. Some companies will actively block known bots and shut down campaigns based on fraud. Others provide scores to advertisers, allowing them to choose how to handle low-scoring campaigns.

There are benefits and drawbacks to both. Integrated systems that automatically stop low-scoring campaigns could end up closing campaigns that have a lot of impression fraud but are also bringing in a lot of revenue. Manual scoring techniques can show where problems exist, but the advertiser must be monitoring this and act quickly to shut down those campaigns before they cause too much damage.

Either way, scoring can be a great way to block known bots from campaigns, especially retargeting campaigns. It can also help companies determine what ad networks and agencies deliver the best results for their campaigns with independent results. That gives you more information to use when making deciding where to allocate your ad budgets in the future.

PROPRIETARY METHODS

There are a number of ad fraud prevention companies that use proprietary algorithms and methods. Because there are no standards for handling or measuring ad fraud, every company deals with it differently. Some are more transparent about how they do things than others, but most will give at least a basic list of attributes and methods used. Common ones include identifying static information, behavioral analytics, and device fingerprinting. Artificial intelligence and machine learning are also used often.

Very few fraud prevention companies can handle every type of ad fraud. Most specialize in recognizing IVT or identifying issues like domain spoofing or ad injection. Though some methods can be layered together for more effective protection, it will depend on the methods used and how they integrate with your ad system. If you choose to layer fraud solutions, you'll want to ask questions about how each product works with others, integration timelines, and how they will impact the speed of your site.

Best Practices for Reducing Ad Fraud

- Pay attention to your campaigns. The only way to spot inconsistencies or major issues is to be looking for them. Watch for any patterns or results that don't make sense based on previous campaigns and general results. Most analytics have ways to do regular reports that can be customized to match the goals and metrics that are most important to your company. By checking these often, you'll be more likely to find issues early.

- Ask questions and look for abnormalities with your ad network or agencies. If they are unwilling or unable to answer basic questions, it could be a sign of a larger problem with that company. In particular, look for companies that have audit tools, clear refund policies, and accept reports from 3rd party verification companies.

- Be wary when things seem too good to be true. Realistically, click-through rates on campaigns are generally low. While a well-crafted campaign can lead to strong conversion rates, it usually takes time to find the right audience and get these results. Too much engagement on social media for a standard ad post that hasn't gone viral could mean that the metrics are being manipulated by bots. Know what a good campaign looks like for your company and be cautious when results are significantly better than normal.

- Don't assume tools are working; check and recheck things often. Too many companies assume that once they have a tool in place, it will just work forever. Fraud is a fast-changing industry that is constantly adapting to current technologies. Even if your defenses are working perfectly today, it's highly likely that someone will develop a new workaround in the future. The only way to ensure continuous protection is to keep up with new changes in fraud prevention.

- Know your customers. Understanding who you are trying to reach will help you position future campaigns to better reach real people interested in your product. Consider things like how your product is used, how popular it is, and how much it costs. A five-carat, platinum diamond ring will have a much different potential customer base than a small silver birthstone ring. If both are getting the same number of highly engaged visitors on your site, it may be a sign that something is wrong. These small considerations can help you filter out bad traffic and focus on increasing conversions.

Ultimately, every company will have a different risk level and defense strategy. To create the best protection for your campaigns, research your options carefully and study your own data. This can help you figure out what the biggest threats are for your company and how you can best protect yourself from them.

About NS8

WE HELP ONLINE BUSINESSES PROTECT THEIR FUTURES

We're passionate about building innovative technology that secures digital transactions and helps our customers safely grow their businesses online. NS8 is a comprehensive fraud prevention platform that combines behavioral analytics, real-time scoring, and global monitoring to help businesses minimize risk. Our patented scoring technology provides actionable data about the type, quality, and trustworthiness of transactions, which businesses can leverage to automate fraud management workflows to suit their individual needs. We also offer supplemental data through third-party extensions as well as seamless integrations with industry-leading ecommerce platforms that enable businesses to begin fighting fraud within minutes.

FUEL YOUR GROWTH WHILE PROTECTING YOUR BUSINESS

Discover how NS8 can help your business eliminate fraud and increase sales and revenue. Schedule a demo with us by calling **+1 (888) 453-5291** or visiting us on the web by clicking below

Request a demo


NS8