RESEARCH REPORT

QUANTIFYING THE COST OF AD FRAUD: 2023-2028

JUNIPER®
RESEARCH

JUNIPER® RESEARCH

Key Findings

22%

AD SPEND LOST DUE TO AD FRAUD IN 2023

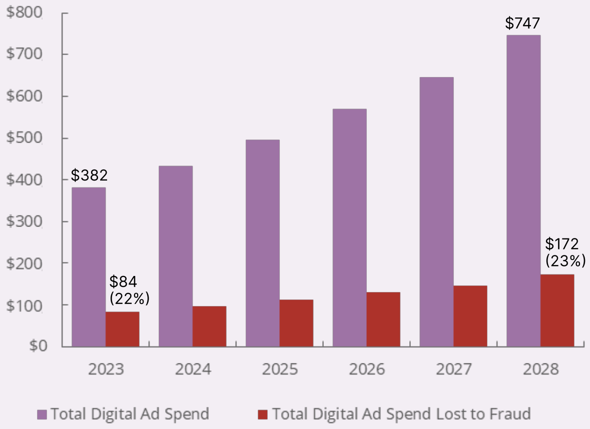
$172B / YR

AD SPEND LOST DUE TO AD FRAUD BY 2028

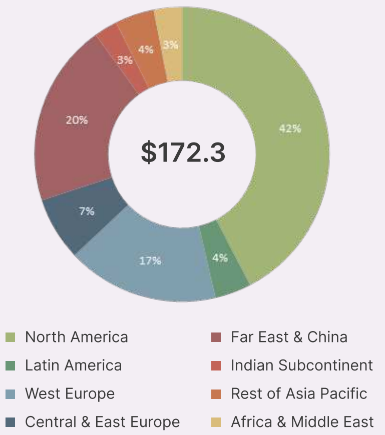
$23B / YR

AD SPEND RECOVERABLE WITH FRAUD MITIGATION PLATFORMS

Total Advertising Spend Lost to Fraud ($B)



Total Projected Ad Spend Lost to Fraud By Country in 2028 ($B)



Methodology

Channels Researched

Online Video Advertising

Online Display Advertising

Online Search Advertising

In-app Advertising

Mobile Browsing Advertising

Social Media Advertising

Data Analyzed

- Analyzed datasets from **78,000 unique sources**
- Reviewed data from **45 countries** in 8 key regions
- Comprehensive data from 6 digital ad channels

**Online Video, Online Display and Online Search Advertising refer to advertising traffic, spend and losses attributable to desktops & PC. In-app advertising refers to ads displayed within mobile apps.*

Table of Contents

CHAPTER 1

THE PROBLEM OF AD FRAUD

JUNIPER® RESEARCH

1. The Problem of Ad Fraud

Ad fraud is a term used to describe any attempt to deceive digital advertisers or digital advertising networks for financial gain. And Juniper Research believes one of the biggest issues facing digital advertisers today is ad fraud. Ad fraud differs from invalid clicks, and is defined as:

"The illegal act of intentionally repeated clicking on PPC (Pay-Per-Click) ads to artificially inflate traffic statistics and generate revenue for illegitimate sources whilst reducing return on ad spend for advertisers."

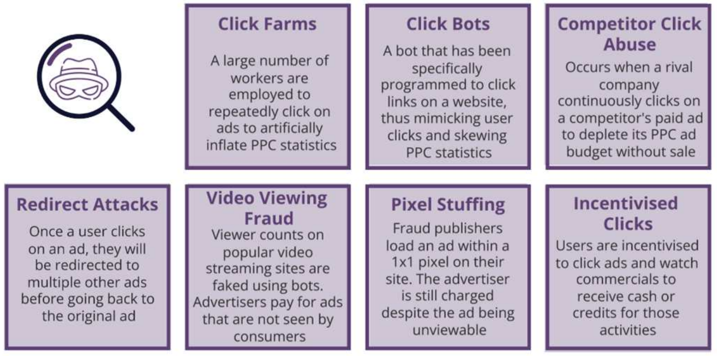
Ad fraud occurs when ads are interacted by a click bot or click farm, for example, so that the publisher makes money at the expense of the advertiser, since the ads are not seen by or clicked on by a potential real user.

Ad fraud impacts advertisers as it diminishes ROAS (Return on Ad Spend), as advertisements are either spoofed by fraudsters or interacted with by invalid users and automated bots. Therefore, advertising and marketing campaigns become less effective, as they are perceived to have a diminished value, thus impacting the use of digital advertising channels.

As highlighted by figure 1.1, there are a number of different types of ad fraud that can significantly impact advertiser return on investment. To combat this, ad fraud mitigation platforms can be deployed to automatically block fraudulent traffic; ensuring an advertiser's ROAS. To do this, a number of tools can be used:

- Monitoring of invalid clicks
- Blacklisting potentially fraudulent devices and IP addresses
- Geolocation tracking
- Real-time detection and blocking
- Customizable criteria for IP blocking
- Managed fraud prevention service

Figure 1.1: Sample Types of Ad Fraud



Click Farms
A large number of workers are employed to repeatedly click on ads to artificially inflate PPC statistics

Click Bots
A bot that has been specifically programmed to click links on a website, thus mimicking user clicks and skewing PPC statistics

Competitor Click Abuse
Occurs when a rival company continuously clicks on a competitor's paid ad to deplete its PPC ad budget without sale

Redirect Attacks
Once a user clicks on an ad, they will be redirected to multiple other ads before going back to the original ad

Video Viewing Fraud
Viewer counts on popular video streaming sites are faked using bots. Advertisers pay for ads that are not seen by consumers

Pixel Stuffing
Fraud publishers load an ad within a 1x1 pixel on their site. The advertiser is still charged despite the ad being unviewable

Incentivised Clicks
Users are incentivised to click ads and watch commercials to receive cash or credits for those activities

Source: Juniper Research

1.1 The Rise of Digital Advertising Fraud

In 2019, Juniper Research predicted that advertisers' total loss to ad fraud would reach $100 billion by 2023. Our projection was very close and based on our calculations today, we expect around $85 billion of advertiser spend will be lost by 2023; rising to almost $100 billion by the end of 2024.

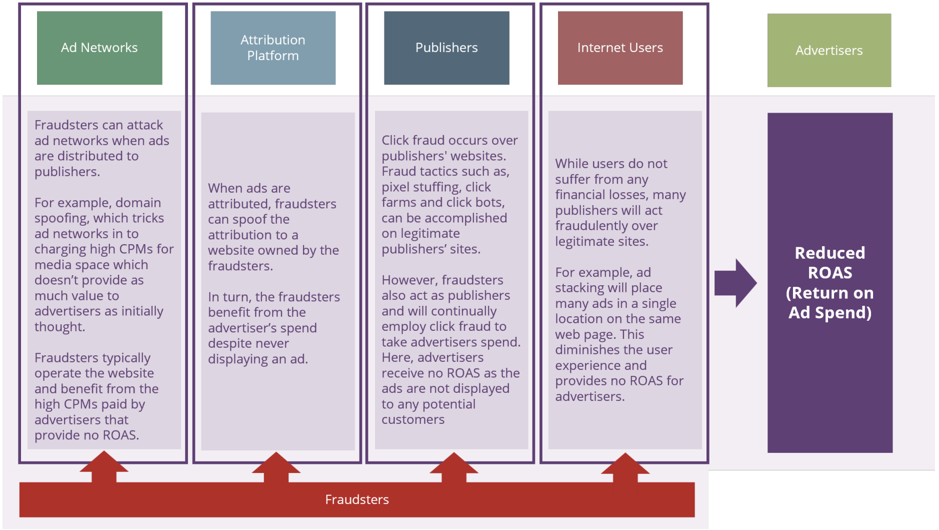
We attribute the deviation in projection to the turbulent economic conditions from COVID-19 that raised caution over the amount of spend used for digital advertising.

Moreover, the behavioral shift following the pandemic has led to digital advertisers becoming more strategic as to where advertising budgets are spent. This strategic use of ad spend means advertisers have now reverted to leveraging third-party fraud mitigation services to ensure their ads are not interacting with invalid traffic; increasing ROAS for advertisers.

1.2 How Does Ad Fraud Work?

Due to the complexity of ad fraud, all parties within the advertising ecosystem, including ad networks, attribution platforms, publishers and even Internet users are susceptible to fraudulent attacks, with all these occurrences resulting in a reduction of ROAS for advertisers. Figure 1.3 highlights how different types of ad fraud impacts different parties during the advertising journey:

Figure 1.3: How Fraud Impacts Each Stage of the Advertising Journey



Fraudsters can attack ad networks when ads are distributed to publishers.

For example, domain spoofing, which tricks ad networks in to charging high CPMs for media space which doesn't provide as much value to advertisers as initially thought.

Fraudsters typically operate the website and benefit from the high CPMs paid by advertisers that provide no ROAS.

When ads are attributed, fraudsters can spoof the attribution to a website owned by the fraudsters.

In turn, the fraudsters benefit from the advertiser's spend despite never displaying an ad.

Click fraud occurs over publishers' websites. Fraud tactics such as, pixel stuffing, click farms and click bots, can be accomplished on legitimate publishers' sites.

However, fraudsters also act as publishers and will continually employ click fraud to take advertisers spend. Here, advertisers receive no ROAS as the ads are not displayed to any potential customers

While users do not suffer from any financial losses, many publishers will act fraudulently over legitimate sites.

For example, ad stacking will place many ads in a single location on the same web page. This diminishes the user experience and provides no ROAS for advertisers.

Source: Juniper Research

1.3 How Click Bots and Fraudsters are Accomplishing Ad fraud

An ad fraud bot is a software program that performs automated malicious activities. Specifically, these bots are programmed to imitate real user activities, with the objective of repetitively clicking on advertisement links. To avoid detection, these bots are often distributed across 'botnets'; a network of connected devices that are used by fraudsters to generate fake traffic to an advert or website.

Notably, each device within a botnet has a different IP address; making it harder for platforms and digital advertisers to detect bot activity. Indeed, both malicious bots and humans can be employed at large-scale click farms, however, in recent years, click farming has moved away from human workers to bots as human click farms require significant set up fees. The use of click bots makes the process cheaper and harder to legislate; distinguishing between legitimate and illegitimate human consumption, as bots can be deployed from multiple devices and IP addresses to avoid detection.

The use of data generated by digital advertising platforms, such as Google and Facebook, is often not sufficient to distinguish genuine user activity from bot traffic. Digital advertisers must form strategic partnerships with ad fraud detection vendors to provide transparent and verifiable data to aid in the identification of illegitimate traffic.

Specifically, Juniper Research acknowledges that the most successful ad fraud detection tools will harness sophisticated machine-learning algorithms to compare consumer behavior with previously observed, verifiable baseline figures whilst also staying vigilant against new and emerging threats. This will enable the accurate detection of supposed users that are actually bots.

Leveraging these services from third-party fraud detection service providers will allow for the swift adoption of these tools; enabling advertisers to filter out malicious bot activity, while also allowing genuine users and 'good' bots to continue interacting with the page or advertisement.

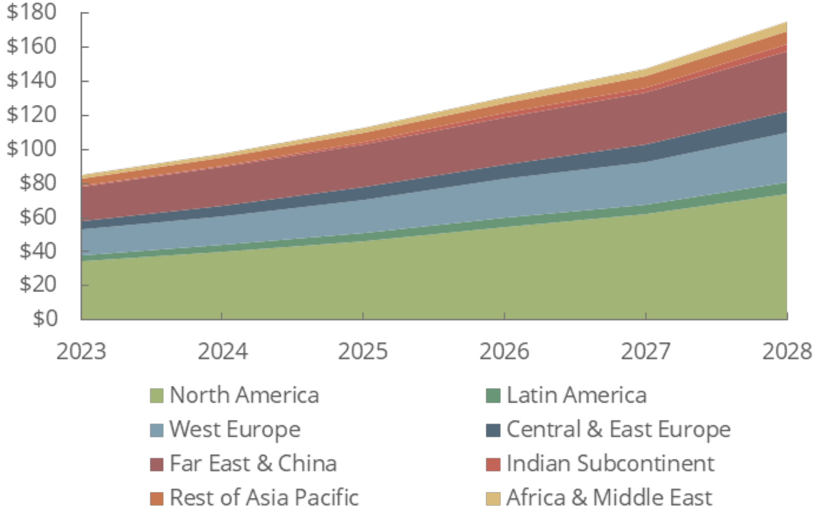
1.4 Global Losses to Ad Fraud

22% of the total value of global spend of digital advertising in 2023 will be lost to ad fraud.

As the digital advertising market is anticipated to grow over 105% over the next five years, this significantly increases the scope and possibilities of ad fraud to occur and intercept advertisers' revenue from advertising efforts. While efforts to tackle advertising fraud increase, the sheer scale of advertising media leaves significant scope for growth in fraud too.

Figure 1.4 highlights the total potential advertising spend that will be lost to fraud in 2023 and the forecasted loss to 2028. Specifically, in 2023, this loss will total $84.2 billion and is anticipated to reach $172.3 billion by 2028. This growth of 105% highlights not only the projected increase in advertisement spend and advertisement loss, but also infers that there will be a significant increase in advertising traffic over the next five years.

Figure 1.4: Total Net Advertising Spend Lost to Fraud, Split by 8 Key Regions, 2023 -2028 (in $ Billions)



North America will account for the highest proportion of advertising spend lost to fraud over the next five years. This market proportion will be driven by North America possessing a mature digital advertising market, which is often used as a testbed by brands and enterprises and is home to a number of key advertising software developers including Amazon, Google, IBM, and Microsoft.

Additionally, Far East and China will deliver a high degree of fraudulent activity between 2023 and 2028. Specifically, by 2028, the region will account for 20% of the global advertising spend lost to fraud. Economies such as China continue to face a click farm pandemic. While the process is moving away from bots to the use of human workers, click farms continue to inflate social currency and can be used in attribution fraud. In order to counteract this, fraud mitigation platforms operating in this country must ensure that their products are able to detect anomalies such as hyper-engagement and short time to install, in order to detect potential instances of click spamming and click injection schemes.

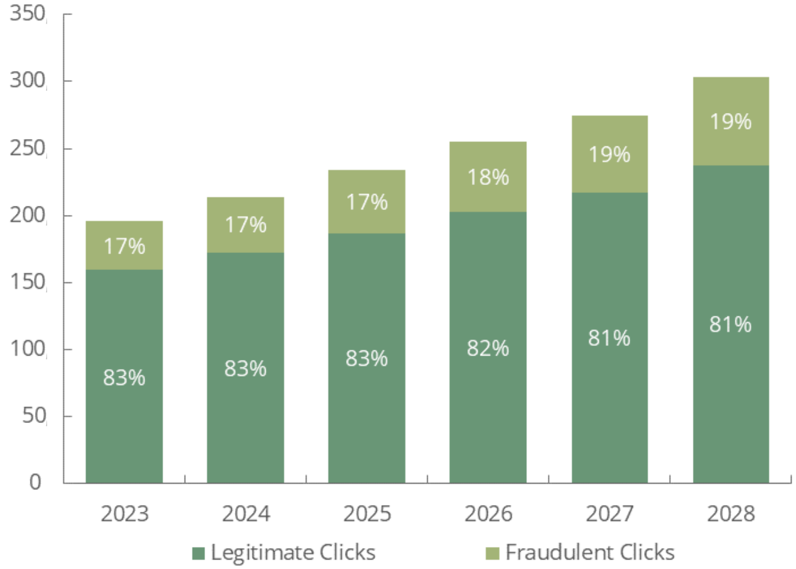
To ensure that the influx of advertising traffic is being sufficiently monitored, fraud mitigation platforms must automate their processes through the use of AI and machine learning. AI software will be able to automatically detect ad fraud through heuristics and pattern recognition, thus ensuring sufficient ROAS for advertisers.

1.5 Total Fraud Transactions

In 2023, Juniper Research estimates that 17% of clickthroughs on PCs and desktops were illegitimate and could not provide ROAS. Despite, the number of legitimate clickthroughs rising from 160 billion in 2023 to over 235 billion by 2028, it is expected that there will be stronger growth of fraudulent traffic; growing from 37 billion fraudulent clickthroughs in 2023 to over 65 billion by 2028.

Moreover, due to digital acceleration during the pandemic, brands and enterprises have widened the scope of channels they service in response to consumer demand for efficient enterprise communication. Therefore, these advertisers must ensure that they protect against ad fraud regardless of channel, as ad fraud impacts all areas of advertising.

Figure 1.5: Total Number of Clickthroughs on PCs & Desktops, Split by Fraudulent & Legitimate, 2023-2028 (in $ Billions)

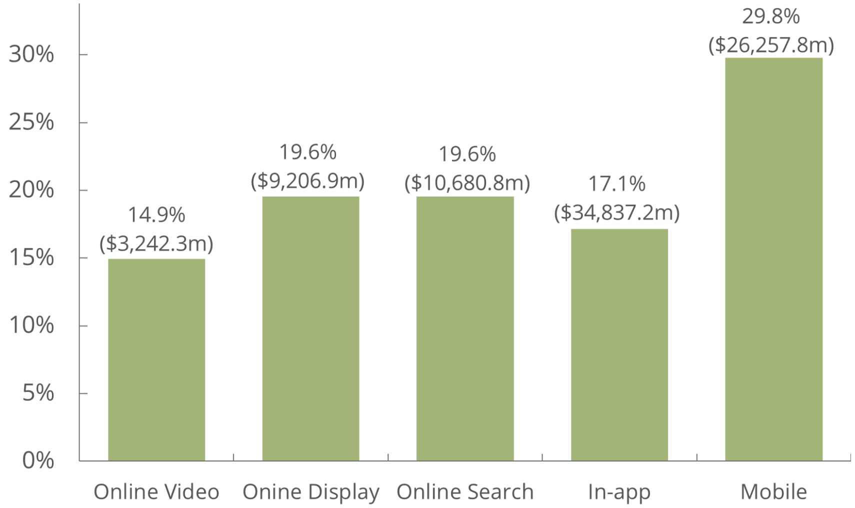


Source: Juniper Research

1.6 Ad Fraud Losses: Channel Assessment

As the availability of Internet access and smartphone usage continues to increase worldwide, Juniper Research notes an abundance of avenues to access; creating a wealth of opportunities for advertisers. However, this also increases the scope of prospects for interception from fraudsters.

Figure 1.6: Proportion of Advertising Spend Lost Due to Fraud in 2023 (%), Split by Advertising Channel



Source: Juniper Research

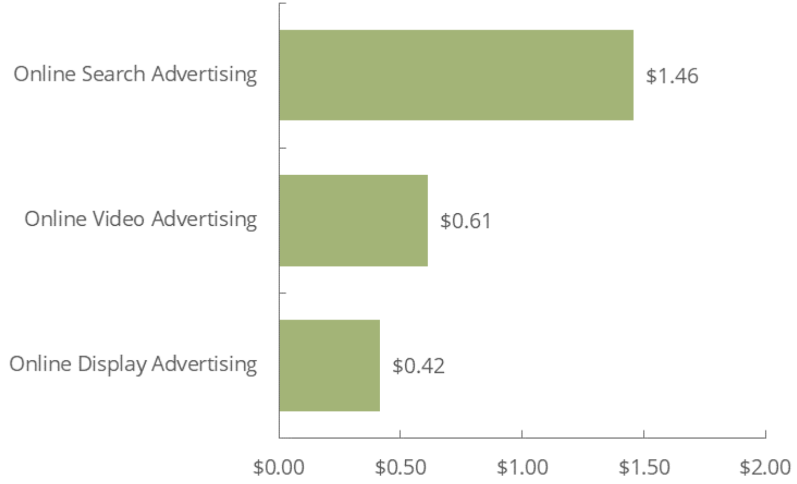
i. Video Advertising

As shown by figure 1.7, the increased average cost of advertising over online video streaming platforms relative to online display advertising will provide an attractive value proposition for both advertisers and fraudsters to capitalize. Specifically, YouTube is the largest video streaming platform service globally when considering the number of users and the reliance on advertising for monetization.

However, it was recently reported that YouTube (owned by Google) has violated its own privacy and anti-fraud policies, as the company has been placing ads in small, muted video players situated in the corner of the screen. It has also been uncovered that Google auto-plays video advertisements on a loop without any viewer interaction or initiation.

While Google denies these accusations, Juniper Research notes that as YouTube is the largest video streaming platform in the world, this scandal by Google will cost advertisers up to $4 billion in advertising spend on video advertising lost to fraud in 2023.

Figure 1.7: Average Equivalent Cost Per Clickthrough for Online Advertising



ii. Online Advertising

Juniper Research anticipates that, of the three online advertising types examined, search advertising will generate the largest fraudulent activity over the next five years. Online fraud is most likely to occur within browsers that have a smaller market share, such as Firefox or Edge, or device-specific browsers, such as Samsung Internet.

With this, search advertising places a specific ad within the search campaign of a consumer. Therefore, it targets a specific consumer with a product or service for which it is actively being searched. Additionally, while online video advertising represents the lowest proportion of online advertising traffic, being expensive compared to display and search ads, they often generate a significantly higher clickthrough rate as consumers are unlikely to ignore them, thus increasing the potential value proposition of using this channel for marketing. However, this increased value proposition does not come without risk as higher clickthrough rates and CPM (cost per thousand impressions) mean that video ads will appeal more to fraudulent players.

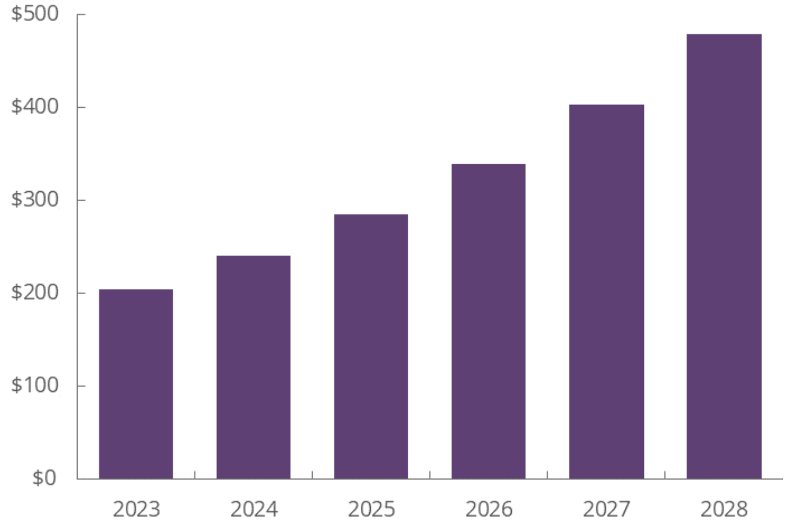
Not only does the type of channel impact ad success, but the type of ad displayed on these channels will also prove important. Advertising channels each provide a different level of ROAS as each channel, ad network, and publisher are open to various levels of fraud. Indeed, advertisers will not always know if their advertisment has been intercepted by fraudulent players until the campaign is complete. Therefore, using fraud detection solutions as a preventative measure before the launch of a campaign will prove vital to ensuring ROAS regardless of channel.

Indeed, browsers with a larger market share, such as Google Chrome and Safari, will have greater built-in security features that will enable the efficient identification and mitigation of fraudulent activity. For example, Google Chrome offers free fraud detection and prevention extensions for its users. However, after the recent misuse of video adverts by Google, Juniper Research notes that advertisers must also invest in additional fraud mitigation solutions to ensure that their adverts are protected regardless of the search engine used.

iii. In-app Advertising

The spend for in-app digital advertising will experience the largest growth over the next five years and is anticipated to increase from $203.8 billion in 2023 to $479.4 billion by 2028; representing a jump of 135%. The reason for this growth is due to consumers increasing the time spent on the apps where these advertisments are embedded.

Figure 1.8: Global In-app Advertising Spend (in $ Billions), 2023-2028



Source: Juniper Research

Additionally, there is a growing divide between ad media supply and demand. With this, ad demand is fast outpacing the supply of media space available, thus driving this increased cost. Advertisers will need to pay more to get their ads displayed on these apps, with additional costs being incurred as the popularity of apps increases. Therefore, this increased advertising spend on in-app advertisements will create many occasions for fraudsters, as this increase means more opportunities to steal ad spend from advertisers.

Advertisers are increasingly using display ads and search ads to trigger app downloads, and therefore higher proportions of subsequent advertisements are being displayed in-app to appeal to this new segment of users. As in-app advertising spend continues to grow, the opportunities for fraudulent activity will also increase and without proper protection, advertisers will be open to increased fraud as in-app advertising spend grows. With this, in-app advertising will generate the greatest ad spend lost to fraud in 2023, and it is anticipated to account for 52% of the global fraud losses by 2028.

Whilst the digital advertising market has reached saturation for some time, the widespread digitalization of multiple industries has led to the emergence of new online platforms and technologies. This has provided a wealth of opportunities for digital advertisers, but has also led to an increase in opportunities for fraudsters.

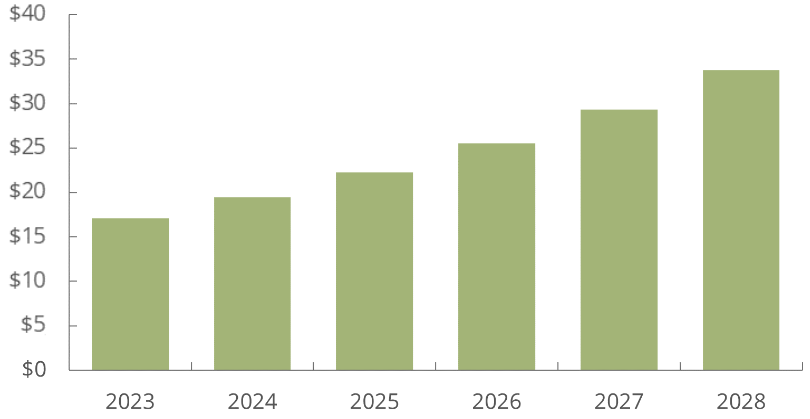
iv. Social Media

Social media is a channel which has undergone a significant transformation in the advertising industry. The primary goal and responsibility of an online advertiser is to create content that encourages users to interact with the company or brand. Indeed, users are often used to interacting and reacting to posts over these social media channels.

Additionally, social media has the ability to infiltrate multiple channels, including in-app advertising, mobile browsing and online display advertising. Therefore, social media advertising services provide a strong avenue to build an interactive relationship with users who have an active presence on social media platforms.

However, as an oligopolistic market, there are only a handful of social media platforms that have a large user base. This means that fraudsters can easily generate targeted fraudulent campaigns that can harm the ROAS of many advertisers over a relatively small number of channels.

Figure 1.9: Global Advertising Losses to Fraudulent Traffic on Social Media Platforms, 2023-2028 (in $ Billions)



Source: Juniper Research

1.7 How AI Is Impacting Ad Fraud

The dichotomy of AI use in the creation and prevention of ad fraud is a topic discussed by many learning fraud mitigation platforms worldwide. Fraudsters can capitalize on the use of AI by using algorithms such as ChatGPT to program advanced algorithms to create bots and malware that can mimic human behavior. Mimicking this behavior allows fraudsters to steal ad spend from advertisers by creating ad impressions and clicks that real users will not see.

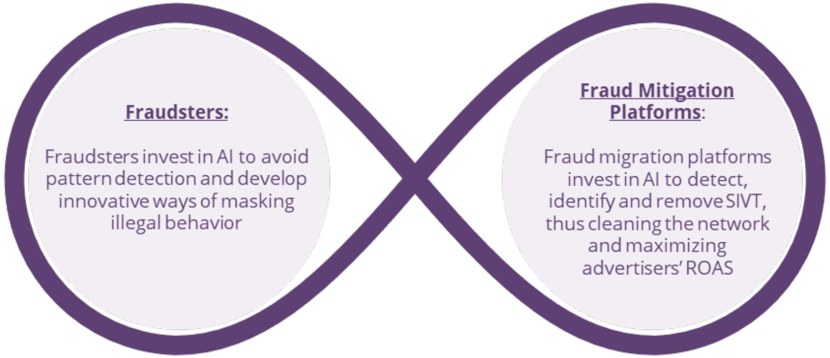
SIVT (Sophisticated Invalid Traffic) is more difficult than GIVT (General Invalid Traffic) to detect because fraudsters are actively changing patterns of attack to avoid detection. To do this, these fraudsters are investing in AI to not only mask their illegal behaviors, but also detect opportunities where they can spoof valid traffic. To combat SIVT, fraud mitigation providers are also having to invest in AI analytics that provide multi-point corroboration to detect, identify and analyze this traffic. However, SIVT (Sophisticated Invalid Traffic) uses AI to actively avoid detection from AI-based fraud mitigating frameworks; creating a 'cat-and-mouse' game involving a form of adversarial AI and resulting in a lack of return on investment for advertisers.

The use of data generated by digital advertising platforms, such as Google and Facebook, is often not sophisticated enough to distinguish genuine user activity from bot traffic compared to third-party fraud mitigation platforms.

Digital advertisers adopt the services from ad fraud detection vendors that are able to provide transparent and verifiable data.

The most successful ad fraud detection tools will harness machine-learning algorithms to compare consumer behavior with previously observed, verifiable baseline figures.

Figure 1.10: How AI Is Impacting Ad Fraud


Fraudsters:
Fraudsters invest in AI to avoid pattern detection and develop innovative ways of masking illegal behavior
Fraud Mitigation Platforms:
Fraud migration platforms invest in AI to detect, identify and remove SIVT, thus cleaning the network and maximizing advertisers' ROAS

Source: Juniper Research

CHAPTER 2

HOW TO MITIGATE THE IMPACTS OF AD FRAUD

JUNIPER® RESEARCH

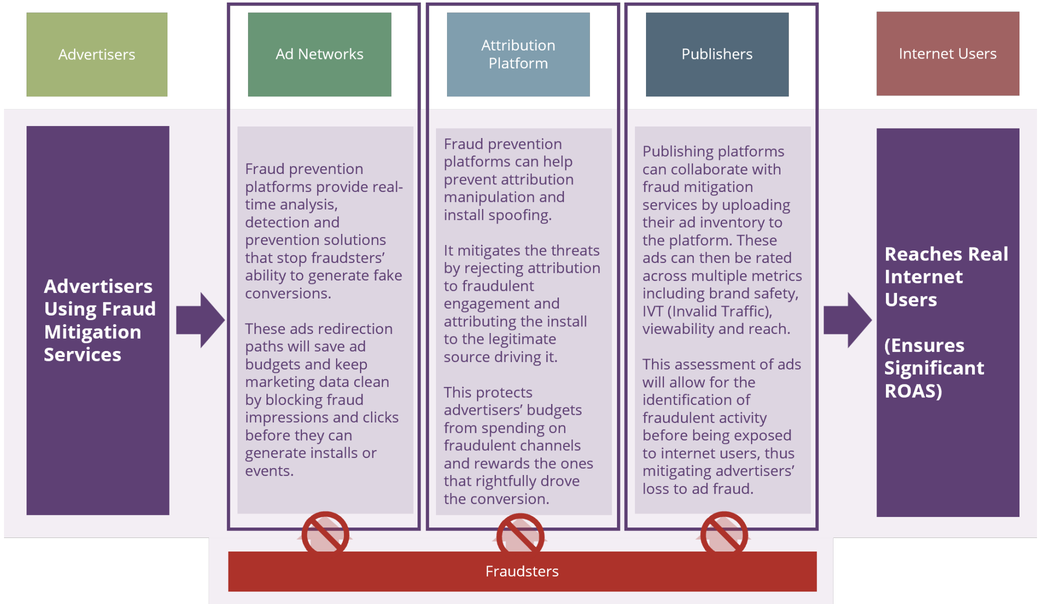
2.1 Fraud Detection & Mitigation Platforms

Data provided by popular ad platforms, such as Facebook and Google, provide an incomplete picture of the success of advertising campaigns. That is, these platforms give an optimistic view of campaign efficiency; failing to distinguish between how many clicks or views originated from legitimate users compared to click farms or fraudulent bots.

As this fraudulent activity will not result in a conversion, this can significantly impact the efficiency of advertising campaigns. To gain a more accurate view into the efficiency of their campaigns, advertisers must implement third-party data analysis tools that combine source data with advanced analytics in order to provide verifiable data.

These third-party data analysis tools are provided by fraud mitigation platforms. As advertisers are the targeted customers of fraud mitigation platforms, this allows these platforms to build an ecosystem whereby the efficiency of machine learning and data-driven algorithms are significantly improved as multiple sources of data are fed through the fraud mitigation systems.

Figure 2.1: How Fraud Mitigation Services Impact Each Stage of the Ad Journey



Advertisers
Ad Networks
Attribution Platform
Publishers
Internet Users
Advertisers Using Fraud Mitigation Services
Fraud prevention platforms provide real-time analysis, detection and prevention solutions that stop fraudsters' ability to generate fake conversions.
These ads redirection paths will save ad budgets and keep marketing data clean by blocking fraud impressions and clicks before they can generate installs or events.
Fraud prevention platforms can help prevent attribution manipulation and install spoofing.
It mitigates the threats by rejecting attribution to fraudulent engagement and attributing the install to the legitimate source driving it.
This protects advertisers' budgets from spending on fraudulent channels and rewards the ones that rightfully drove the conversion.
Publishing platforms can collaborate with fraud mitigation services by uploading their ad inventory to the platform. These ads can then be rated across multiple metrics including brand safety, IVT (Invalid Traffic), viewability and reach.
This assessment of ads will allow for the identification of fraudulent activity before being exposed to internet users, thus mitigating advertisers' loss to ad fraud.
Reaches Real Internet Users
(Ensures Significant ROAS)
Fraudsters

Source: Juniper Research

This allows for a blacklist to be created which stores the IP addresses, publisher IDs, and device IDs among other criteria that have been detected committing fraudulent activity over ad networks.

This is beneficial for advertisers as they will have access to a well-informed, real-time blacklist that automatically monitors and blocks known fraudsters. However, it is important for advertisers to choose a fraud mitigation platform that is constantly analyzing these channels for new sources of fraud or emerging fraud tactics.

This will enable the accurate detection of supposed users that are actually bots or click farms. Adoption of these tools will allow digital advertisers to filter out malicious bot activity, whilst also allowing genuine users and good bots' continued interaction with the page or advertisement. As malicious ads can then be blocked in real-time, this will save significant ROAS for advertisers.

While ad fraud can impact brands and enterprises of any size, given the smaller marketing budgets of SMBs (Small-to-Medium Businesses), it is more important for these companies to maximize ROAS. Additionally, as these businesses are unlikely to have the in-house expertise to mitigate ad fraud attempts, Juniper Research anticipates that these businesses will leverage solutions and expertise of third-party solutions of fraud mitigation platforms to automatically identify and block fraudulent clicks.

Indeed, Juniper Research also forecasts that the global potential advertising spend lost to fraud will rise from $84 billion in 2023 to $172 billion by 2028. This growth of 105% highlights the urgency for deploying innovative fraud mitigation services such as IP monitoring, VPN (Virtual Private Network) detection, geolocation tracing, fraud scoring and blacklisting to combat the sophistication of ad fraud and SIVT.

As these fraud mitigation platforms can save advertisers on wasted ad spend, investing in these services is fundamental to ensure that advertisers are not a target of ad fraud. It will also ensure that advertisers can maximize their ROAS and not contribute to the $172 billion of advertising spend lost to fraud by 2028.

Specifically, Juniper Research forecasts that **fraud mitigation platforms will recover over $23 billion of advertiser spend lost to fraud in 2023, with this figure rising to over $47 billion by 2028.**

CHAPTER 3

FRAUD BLOCKER

JUNIPER® RESEARCH

3.1 Fraud Blocker, Leading Ad Fraud Protection Software

Fraud Blocker provides an all-in-one solution that **improves ad performance** by analyzing, detecting and preventing ads from appearing to bots, competitors and other malicious sources.

Today, the company protects over 4,000 websites and analyzes over 500,000 unique IP behavior daily to ensure that advertisers are not wasting ad spend on fraudulent and invalid ad traffic.

Figure 3.1: Awards and Recognition

Momentum Leader FALL 2023
High Performer FALL 2023
Easiest To Do Business With FALL 2023
High Performer Americas FALL 2023
TOP AD FRAUD DETECTION COMPANIES Business of Apps 2023
APPSUMO
★★★★½
★★★★½

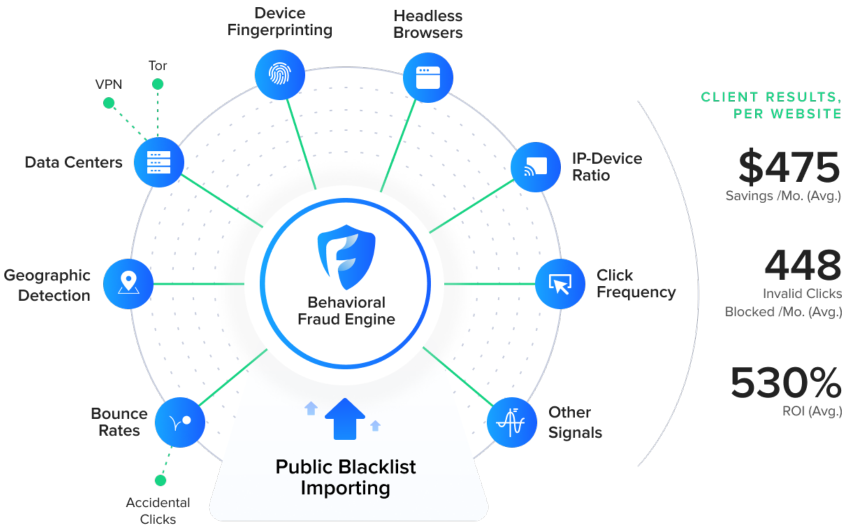
Fraud Blocker blocks sources of fraudulent ad traffic by monitoring inbound web visitors to an advertiser's website and looking for irregular behavior from the source that could suggest it's from a bot, non-human source, click farm, competitor, accidental clicks, and more.

This analysis includes tracking a web visitor's IP address and device fingerprint, and reviewing dozens of signals in real-time such as bounce rates, IP-to-device ratios, VPNs, click frequency, etc.

Once an invalid or low quality user is detected, Fraud Blocker automatically prevent ads from being served to them, thus saving customers money while also improving their ad performance.

Figure 3.2 shows the wide-range of detection methods Fraud Blocker users to analyze a source for fraud. On average, their customers see significant ROI improvement by preventing invalid clicks and increasing the quality of their traffic flow.

Figure 3.2: Key Benefits of Fraud Blocker's Detection Platform



Source: Fraud Blocker

Fraud Blocker Contact Information

Website & pricing: fraudblocker.com
Product demo: fraudblocker.com/demo
Email: info@fraudblocker.com

APPENDIX

ABOUT JUNIPER RESEARCH

JUNIPER® RESEARCH

About Juniper Research

JUNIPER® RESEARCH

Juniper Research was founded in 2001 by industry consultant Tony Crabtree in the midst of the telecoms and dot-com crash. The business was fully incorporated in February 2002 and has since grown to become one of the leading analyst firms in the mobile and digital tech sector.

Juniper Research specializes in identifying and appraising new high-growth market sectors within the digital ecosystem. Market sizing and forecasting are the cornerstones of its offering, together with competitive analysis, strategic assessment and business modeling.

The company endeavors to provide independent and impartial analysis of both current and emerging opportunities via a team of dedicated specialists - all knowledgeable, experienced and experts in their field.

Its clients range from mobile operators through to content providers, vendors and financial institutions. Juniper Research's client base spans the globe, with the majority of its clients based in North America, Western Europe and the Far East.

For more information about Juniper Research, please see: juniperresearch.com/home