The State of Fake Traffic

2023

CHEQ

Table of contents

Introduction

What is Fake Traffic?

Over the past 40 years, the internet has expanded into a massive highway of information–with billions of daily active users, and trillions of daily engagements – driving innovation, growth, and connectivity on a global scale.

But as the internet has grown in scale and sophistication, the quality and authenticity of its traffic has decreased, leaving the web flooded with automation tools, bots (good or bad), and users who, for one reason or another, aren't genuine. In the business world, this traffic is known as fake traffic.

Fake traffic is web traffic that consists of bots, fake users, and otherwise invalid users that cannot turn into a legitimate customer. This could mean harmless bots like a search engine's crawlers, or malicious traffic like ad fraud botnets.

Research has revealed that upwards of 40% of all traffic* online is invalid, though not all of that traffic impacts businesses. In this report, we examine the invalid traffic affecting businesses and consumer-facing websites.

For marketers, fake traffic is a concern because it wastes valuable advertising dollars, pollutes funnels with invalid leads, and ultimately skews analytics used to make critical decisions.

But the effects of fake traffic extend far beyond the marketing department–the Fake Web has become a strategic business issue.

Entire organizations from Twitter, to PayPal, to Ticketmaster, and everyone in between, have had to jump into crisis mode after go-to-market initiatives unintentionally led to exploitation from bad actors on the web. This report will cover the issues and implications for business operating today in this era of fake traffic.

*Wired.com, 2022

Introduction

The Impact on Go-to-Market Organizations

Historically, fake traffic has been the domain of IT and security teams, and its impact on go-to-market organizations have largely been overlooked. However, as today's C-suite has realized, fake traffic is a prevalent problem for go-to-market teams and can threaten the overall security of a business.

For marketers and businesses dependent on web traffic to drive sales, this creates a unique challenge: Because of the prevalence of fake traffic, nearly every funnel, campaign, and operation is impacted to some degree, oftentimes in very harmful ways.

Where fake traffic is present, audiences, CDP segments, and CRMs become polluted, campaigns become optimized toward fake users, and revenue opportunities are missed. Analytics and BI systems are skewed by bad data, leading to poor insights and worse, decisions made on bad information.

Additionally, website and conversion funnels are disrupted by invalid leads and visitors. This is a challenge that must be dealt with, sooner, rather than later.

That's why in this report, we want to show you just how widespread and pervasive the threat of fake traffic is. Using data from thousands of websites and billions of valid and invalid visits from 2022, we examined the prevalence of the different threat types that make up fake traffic, how fake traffic adversely affects various industries, countries, and regions, and how fake traffic breaks down across marketing channels.

We'll also use this data to build predictions about the state of fake traffic in 2023, and how marketers and security teams can best adapt to overcome this growing challenge.

"Where fake traffic is present, audiences, CDP segments, and CRMs become polluted, campaigns become optimized toward fake users, and revenue opportunities are missed."

Executive Summary

In 2022...

We evaluated the invalid traffic rates of over 15,000 CHEQ customers and discovered that the volume of blocked fake traffic increased at an unprecedented level, up **167%** from 2021.

11.3%
Of all traffic was fake

5.9%
Of paid traffic was fake

5.7%
Of organic traffic was fake

22.1%
Of direct traffic was fake

Additionally, over the course of the last year:

1 in 10
Website visitors was inauthentic

1 in 50
Visitors had malicious intent

$35.7B
of ad spend was wasted

$142.8B
in revenue was lost

Executive Summary

Growing Threats

The growth of fake traffic in 2022 was broad across all threat types and attack vectors, but three threats increased more than the rest:

125%
Click Hijacking attacks grew

112%
Malicious Bot attacks grew

101%
Web Scraper attacks grew

Most Impacted Industries

Fake traffic affects every industry with a web presence, but three in particular were hardest hit.

These are the invalid rates for the industries most targeted by fake traffic.

49.1%
Gaming and Gambling

20%
Tech/SaaS

17.3%
Telecom

Methodology

As the global leader in Go-to-Market Security, CHEQ frequently studies activity originating from various direct, organic and paid traffic sources on the web to determine whether or not each site visitor is a bot, malicious user, or human with legitimate interest.

The inaugural State of Fake Traffic report study was conducted over an entire year analyzing data from more than 15,000 CHEQ customers. When a user arrived on a domain owned and operated by these customers, CHEQ performed more than 2,000 real-time cybersecurity challenges to determine each visit's validity or lack thereof.

Traffic determined to be invalid or malicious was blocked or redirected before it could negatively impact customers.

After categorizing the traffic, we broke down the fake traffic rates by traffic source (direct, organic, paid), industry, geolocation, and threat type.

The goal of this study was to analyze fake traffic activity across the internet in order to provide actionable insights and guidance on the characteristics, effects, and threats posed by fake traffic.

We then used these fake traffic rates, combined with external metrics, to calculate the impact fake traffic has on marketing-generated revenue, sales operations, and BI-driven decision-making.

Fake Traffic Threat Groups

We tracked three broad categories of threats as well as several specific threat types.

Suspicious Activity

Suspicious traffic comes from users that have one or more characteristics that identify them as a threat. Suspicious traffic may be from data centers or users who hide behind proxies, VPNs, and false identities. In 2022, suspicious activity made up **44.3%** of all fake traffic, more than doubling from 21.8% in 2021.

Bot Activity

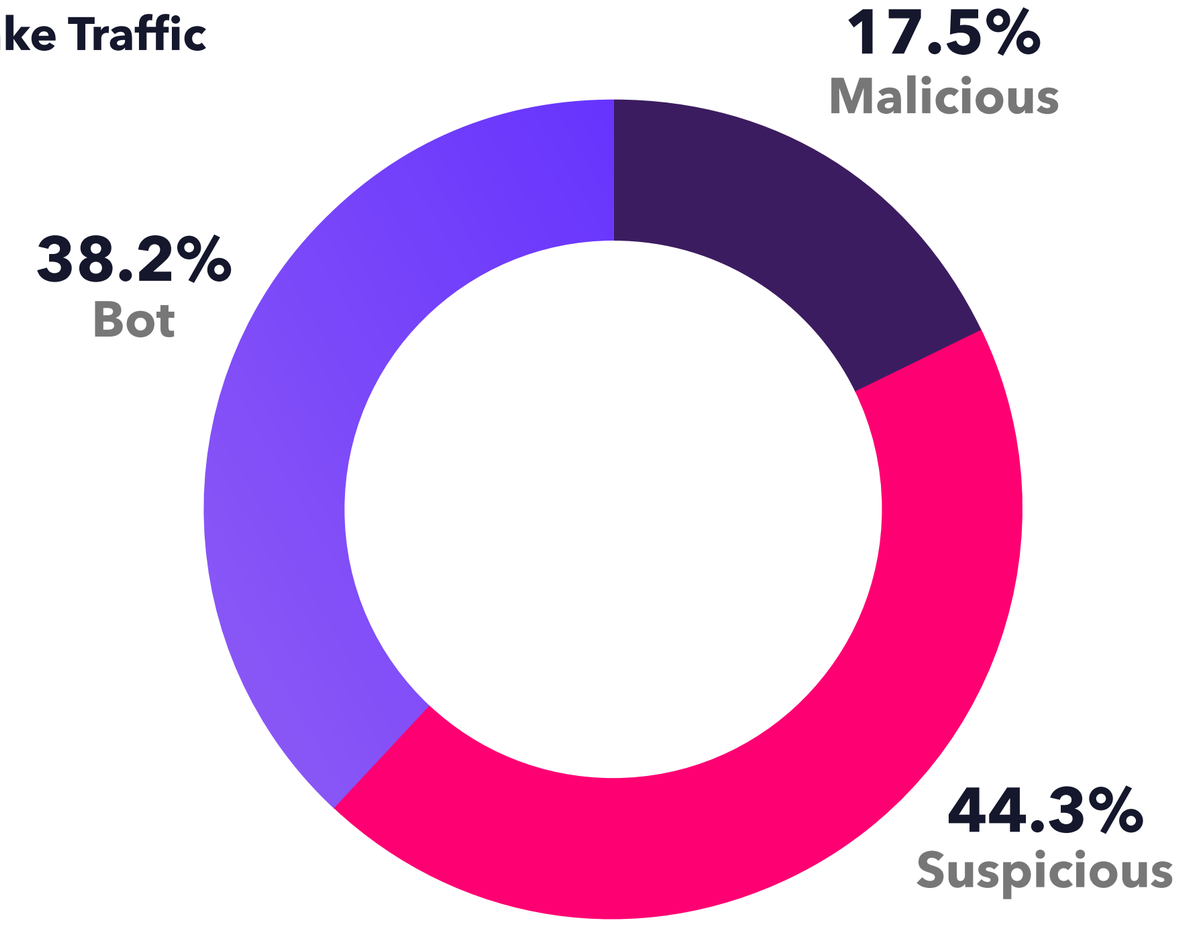
From Elon Musk's crusade against Twitter bots, to bots shutting down a Taylor Swift tour and enrolling in Universities to secure bogus student aid claims, bots were all over the news in 2022.

A bot is an automated tool or system that performs automated predefined tasks. Bots can imitate or replace human user behavior, and can be used for malicious purposes, such as Distributed Denial of Service (DDOS) attacks or ad fraud. In 2022, invalid bot activity made up **38.2%** of all fake traffic, an increase from 30.1% in 2021.

Malicious Activity

A malicious user creates fake activity purposefully with harmful intentions. Often, malicious users are looking for easy targets for card skimming or account takeover attacks. In 2022, overtly malicious traffic comprised **17.4%** of all fake traffic blocked by CHEQ, and 2% of all examined traffic. Meaning that one in every 50 visitors to a given website has malicious intent.

Threat Groups as a Percentage of All Fake Traffic



Threat Groups

Types of Fake Traffic

Threat Groups and Types

To gain a nuanced understanding of the threats posed by fake traffic, CHEQ categorizes the vast ecosystem of invalid traffic threats into over 20 distinct threat types. The chart below details the ten most prevalent threat types in 2022 as a percentage of all invalid traffic. Automation tools--bots used to perform routine tasks such as web indexing or SEO evaluation--made up the largest portion of fake traffic at **20.1%**.

While these tools are often benign, they can not convert or complete real actions and should be filtered out of marketing data and analytics. When comparing threat data to data collected in 2021, we identified three rising threats that grew exponentially in 2022: click hijacking, malicious bot attacks, and web scraper attacks.

Top Threats of a Percentage of All Fake Traffic, 2022

Other is comprised of Low Quality Users, Geo Exclusions, Disabled Cookies, and other suspicious behaviors.

Threat Groups

Growing Threats

Click Hijacking Attacks

Click hijacking saw an exponential increase in 2022, growing **125% year-over-year** up to **16.6%** of all fake traffic.

Click hijacking occurs when a valid user clicks on an asset, such as a link or advertisement, that appears to be legitimate, but it is actually a disguised malicious element, which may install malware, or redirect users. Last year, researchers discovered a set of Google Chrome extensions that had been installed over one million times was hijacking searches and inserting affiliate links into web pages, disrupting user experience, and costing retailers thousands in affiliate fraud.

Malicious Bot Attacks

Malicious bot attacks increased **112% year-over-year,** up to **8.1%** of all fake traffic in 2022. These are known bots specifically designed to carry out attacks such as card skimming, price scalping, account takeover attacks, ad fraud, and data theft.

Scalper bots, which snap up online inventory faster than any human ever could, only to relist the products for inflated prices elsewhere, saw a particularly high increase in the holiday shopping season, culminating in a run on Taylor Swift tickets that took Ticketmaster offline and ended in lawsuits and even a Congressional hearing.

Web Scrapers

Instances of blocked web scrapers increased **101% year-over-year**, making up **9.1%** of all fake traffic in 2022. Web scrapers are bots that scan websites looking for a specific target or piece of data. This frequently occurs on e-commerce websites with the intention to find prices to then sell items for slightly less and therefore gain more customers than the competition.

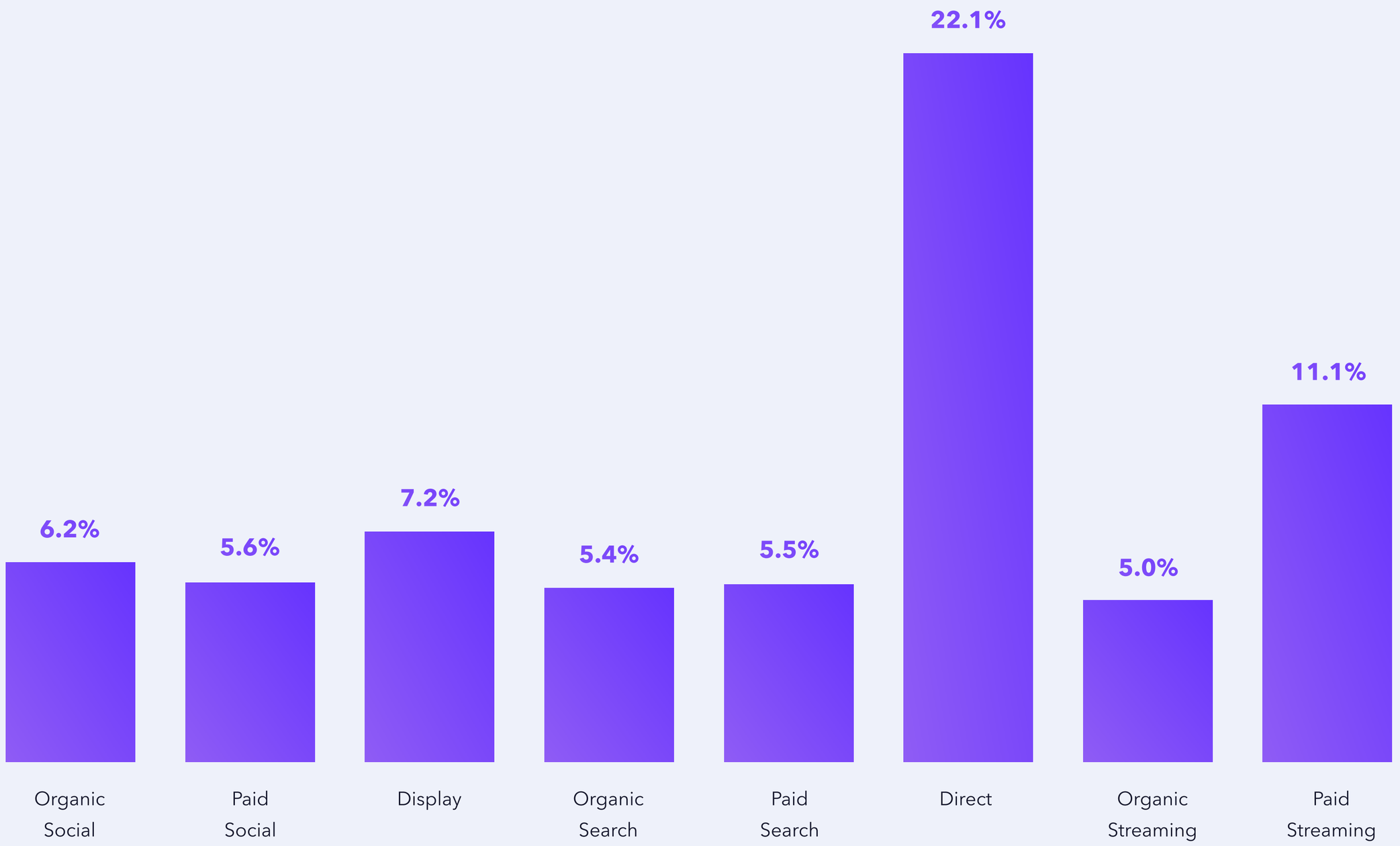
"Click hijacking saw an exponential increase in 2022, growing 125% year-over-year up to 16.6% of all fake traffic."

Fake Traffic by Source

Fake traffic is a persistent threat that affects all digital marketing channels. Left unaddressed, this fake traffic will waste advertising budgets and create negative downstream effects such as poorly optimized and ineffective campaigns, confused analytics, and inaccurate attribution. Despite the best efforts of search engines, ad networks, and social media platforms to mitigate fraud and falsification through dedicated teams and built-in tools, there remains a significant ingress of fake traffic across all platforms.

Our analysis of billions of fake traffic referrals found a general level of parity in fake traffic across most platforms, with some notable exceptions. The general findings of our research is outlined in the chart below, with detailed examination of the data in the following pages.

Fake Traffic Rates by Referral Source, 2022



Social Fake Traffic Rates Climb as Professional Networks Attract Bad Actors

While the general fake traffic rates for social media platforms were lower than comparable search and display ads, one category of social media had, by far, the highest fake traffic rates of any platform studied.

Professional networking platforms had an average invalid referral rate of **12.4%**, with **9.7%** of paid traffic and **15.3%** of organic traffic determined to be invalid.
For hackers, these platforms make a convenient group of high-value targets.

For those committing ad fraud, the incentive is even stronger. At an average of $5.58 per click in 2022, the cost-per-click for professional networks is typically up to five times that of typical social and PPC costs. From an attacker's point of view, that makes it five-times more efficient to target a campaign on these sites.

Twitter: The Biggest Bot Story of 2022

Twitter certainly got the most bot-based negative attention of any social-media platform in 2022, but with an average **5.3%** fake traffic rate (from a weighted average of paid and organic referrals),the company did not fare particularly poorly compared to its peers. Throughout the year, however, Twitter did generate several large spikes in invalid referrals, notably in May, when Mr.Musk paused his acquisition of the company due to concerns over fake accounts; in October, when the deal was forced through, and in December, when Musk announced an increased crackdown on bots and fake accounts.

Click Hijacking Attacks Drive Fake Traffic to Display Ads

Display ads are the oldest form of online advertising, and they're still an extremely effective tool that allows businesses to reach a broad audience and raise brand awareness. However, because they are delivered to third-party websites and can be easily manipulated by malicious actors. Display ads are particularly vulnerable to clickjacking attacks, which grew by 125% across all platforms in 2022. This deluge of attacks lead to a fraud rate of **7.2%** for displays in 2022, **40%** higher than the rate for search ads. In a click hijacking attack, an attacker will use various techniques, such as adding hidden layers or modifying the code of a webpage, to cause a display ad to be clicked without the user's knowledge. The attacker can then collect payment for the fake click from the advertiser.

This type of attack can be difficult to detect and prevent because it occurs on the client side, and the user's browser is often not able to distinguish between a legitimate click and a hijacking click.

Viewbots Inflate Streaming Numbers and Burn Advertising Dollars

Streaming platforms had an unprecedented reach in 2022. The top streaming site reaches more people aged 18-49 than all TV networks combined, and it reaches them with more ads–which are statistically more likely to hold viewer attention, and ultimately to convert.

But many of those ad viewers are not human. In 2022, streaming platforms generated the highest invalid rate for paid traffic of any category, at **11.1%**. Based on the ad revenue figures of just one streaming platform, that could amount to over **$3 billion in wasted ad spend.**

So where is all of this traffic coming from? The answer is view bots, a relatively new form of fake traffic in which pieces of automated software (bots) are used to view streaming videos or live streams in order to artificially boost the view count and generate fake engagement–and fake ad views–for unscrupulous creators.

Most view bots are simple scripts that open a video in a headless browser, but more complicated viewbots may also create fake accounts to mimic logged-in viewers, and can even incorporate a chatbot capability that will spam the stream's chat or comments section with artificial banter to make audience numbers appear more legitimate. Some viewbots will even click through on ads to increase the perceived click-through rate. And these bot networks are available for rent for prices as low as $10/month.

The impact of these fake viewers goes far beyond fake clicks–most established creators offer partner programs, where they earn a commission for mentions or ad impressions. If those impressions are generated by bots, not real people, then the ad budget used to create and place those ads has essentially been wasted.

If it costs $2000 for 100,000 impressions, and 15-20% of those impressions are fake, that's $150-200 wasted. Considering most advertising campaigns on these platforms measure impressions in the millions, the costs of those fake impressions can add up fast. Furthermore, with key performance metrics becoming skewed by fake traffic, decision making becomes increasingly difficult.

Fake Traffic Across Industries

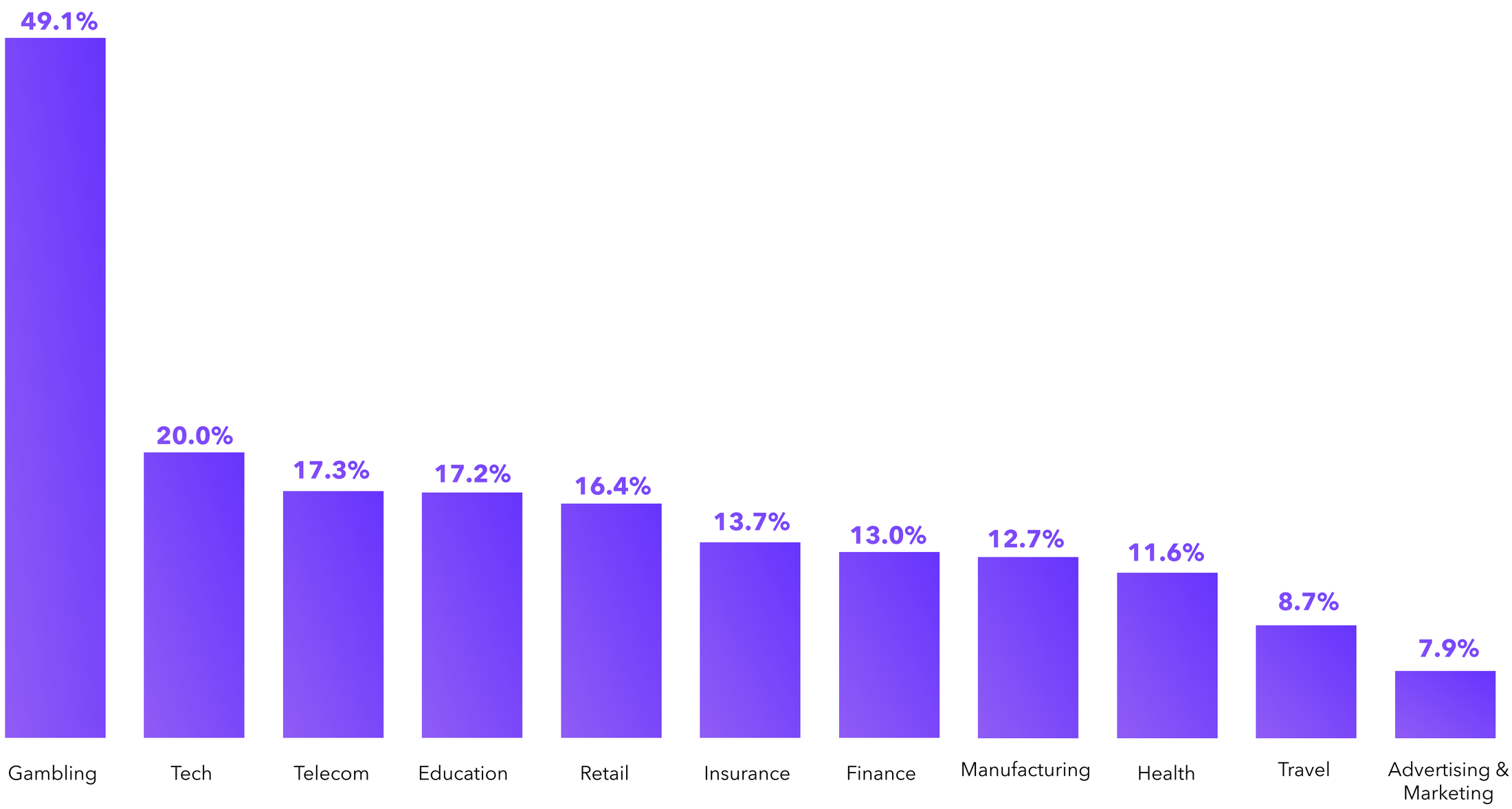
Fake traffic is a pervasive threat that affects any business businesses of all sizes, across all industries. While industries that rely on online traffic or advertisements as a source of revenue face a higher risk of ad fraud, any unprotected site is a potential target for hackers and bad actors.

Our analysis of data from a range of clients across various industries showed that the industry in which a business operates can significantly impact its level of fake traffic.

The **Gambling & Gaming** industry experienced the highest rates of click fraud in 2022, with **49.1%** of gross traffic deemed invalid.

Tech, Education, and Telecommunications also saw above average rates of fraud in 2022. In the following pages we will examine which threat types adversely affected each industry.

Fake Traffic Rate by Industry, 2022



Fake Traffic Across Industries

Advertising and Marketing

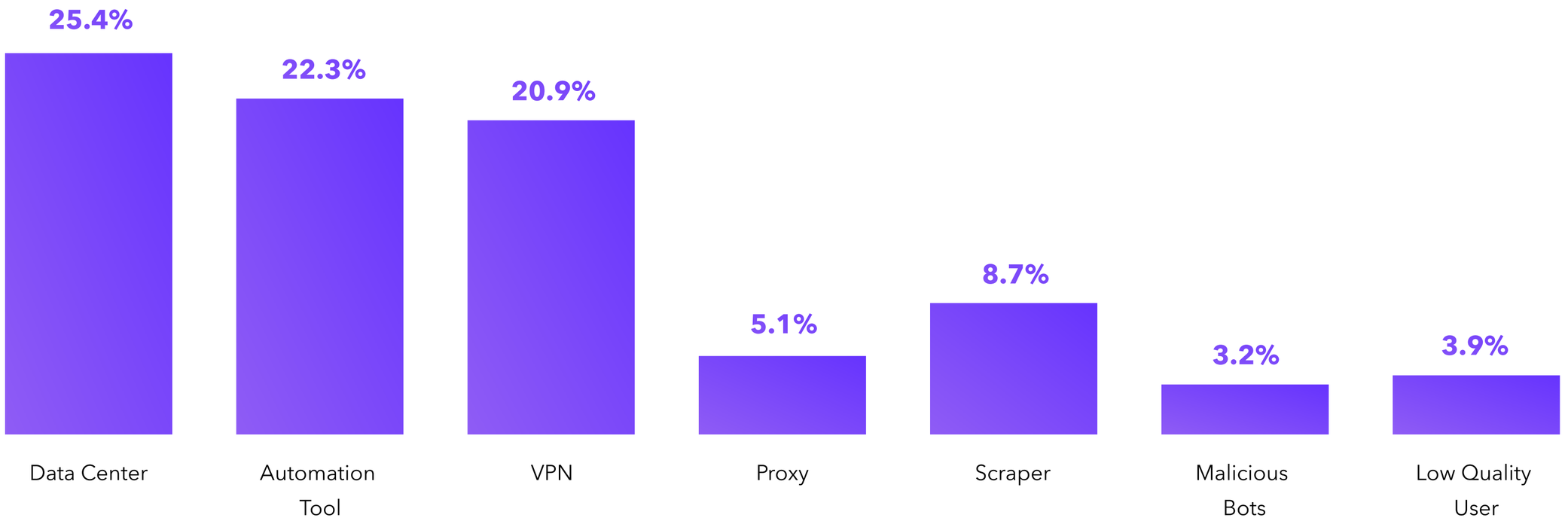
Fake traffic attempting to access Advertising and Marketing websites amounted to **7.9%** of all site traffic. The majority of the fake traffic discovered and blocked by CHEQ originated from data centers and automation tools.

The advertising industry is a favorite target of click farms and botnets used to carry out ad and affiliate fraud, but those attacks are largely concentrated on ads and content hosted on third party platforms, and thus do not figure into these results.

For advertising and marketing agencies, the risk of fake traffic poses a double threat, encompassing both a potential threat to ad revenue, and a reputational threat for firms managing client's campaigns.

7.9%	4.9%	7.5%	5.7%
Overall	**Paid**	**Direct**	**Organic**

Threat Types as a percentage of Total Fake Traffic, Advertising and Marketing, 2022



Fake Traffic Across Industries

Tech and SaaS

The software-as-a-service (SaaS) market is expected to be worth over $200 Billion by 2023, according to research from Statista, and that value has been largely been built by B2B tools that take complex business processes, simplify them, and make them readily available online, enabling remote work, collaboration, and efficiency.

But that same business model has made SaaS tools and companies a potential treasure trove for hackers–the successful breach of a single SaaS tool could mean access to the sensitive data of thousands of client businesses. Behind Gambling, SaaS companies had the second highest rate of fake traffic at **20%** in 2022.

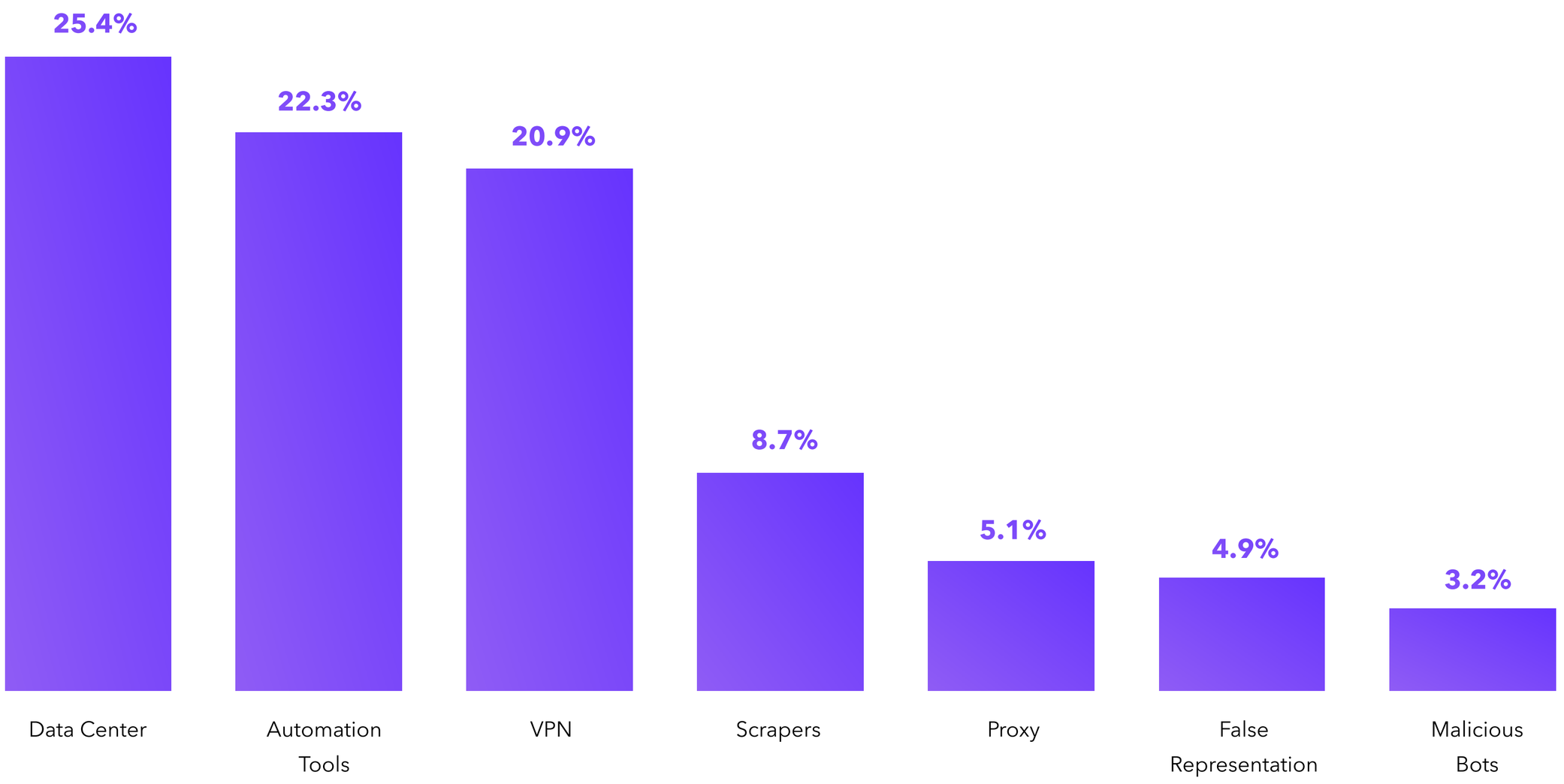
20%
Overall

5.9%
Paid

8.8%
Organic

23.4%
Direct

Threat Types as a Percentage of Total Fake Traffic, Tech and SaaS, 2022



Fake Traffic Across Industries

Learning and Higher Education

Colleges made headlines in 2021 when it was discovered that bots and fake users had been signing up in (often successful) attempts to receive student aid and benefits, and it appears that Higher Education's bot problem persisted in 2022.

In the last year, 17.2% of traffic to CHEQ-protected websites in the education sector was invalid, with an excessively high invalid rate for direct traffic at 32.9%, and a higher than average amount of blocked malicious bot attacks indicating a continued interest from bots and fraudsters.

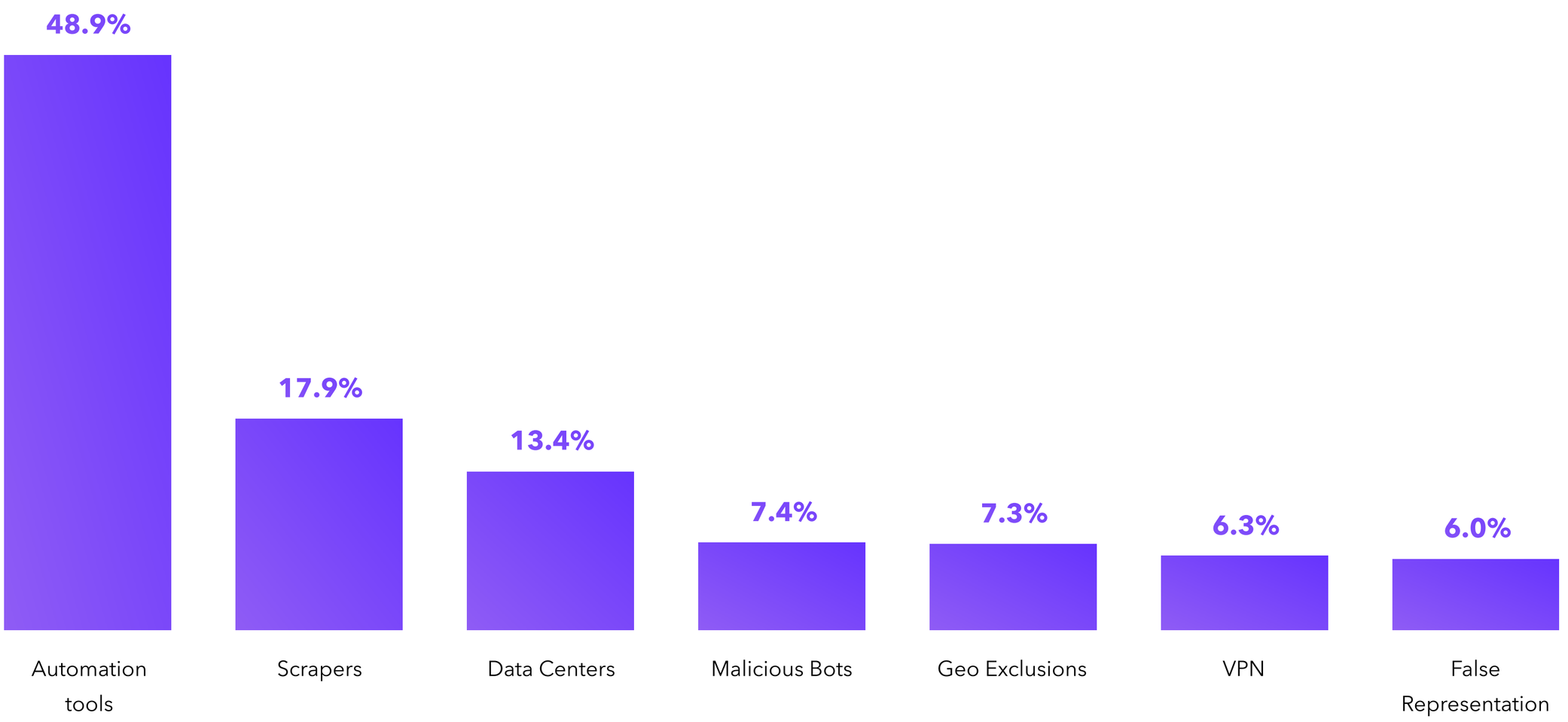
17.2%
Overall

4.5%
Paid

32.9%
Direct

8.2%
Organic

Threat Types as a Percentage of Total Fake Traffic, Learning and Higher Ed, 2022



Fake Traffic Across Industries

Finance

Following the 2017 Equifax data breach and increased scrutiny from regulators at home and abroad, most finance and fintech businesses have taken a hardened security posture against attackers, but that doesn't mean the attackers have lost interest.

In 2022, the finance industry had an average fake traffic rate of 13%, with particular interest from web scraper tools, which made up approximately 1.3% of all traffic to finance sites.

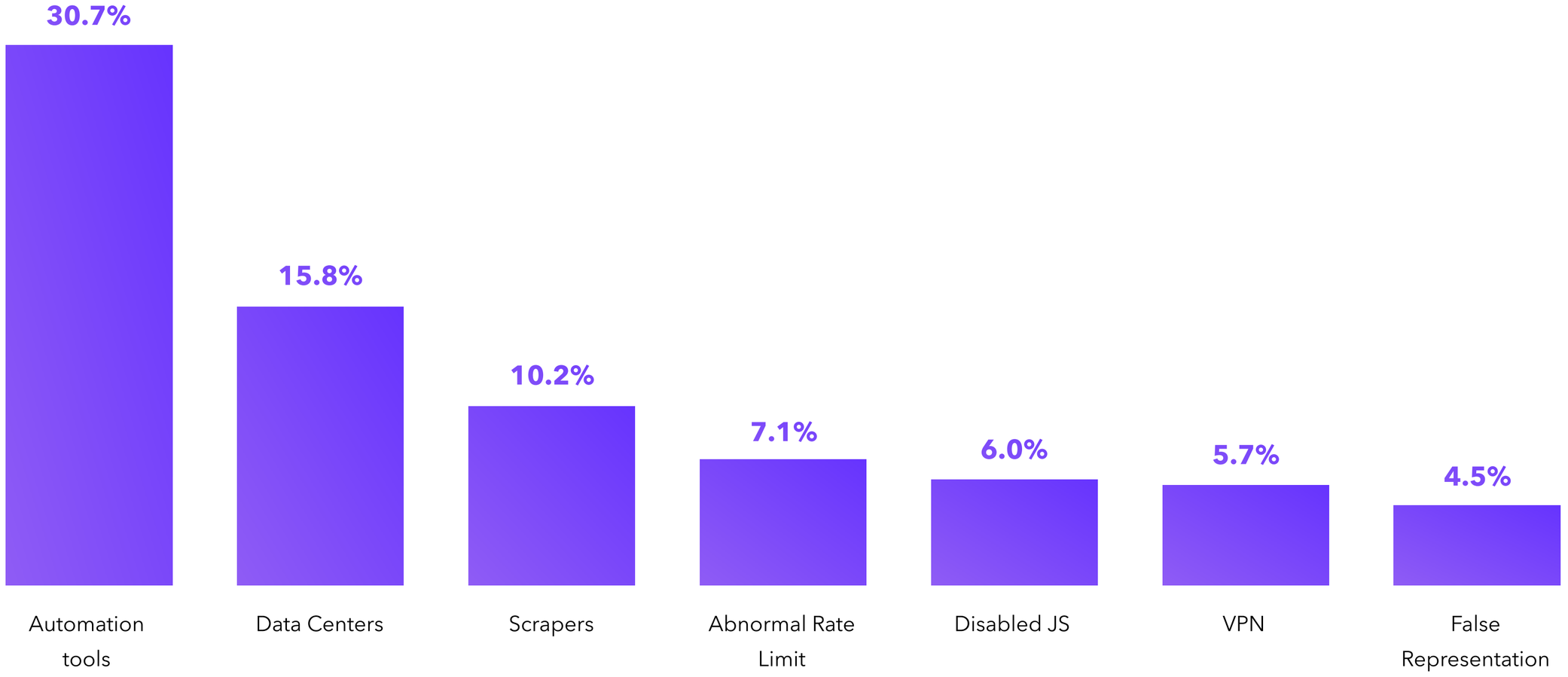
13%
Overall

3.1%
Paid

19.7%
Direct

4.9%
Organic

Threat Types as a Percentage of Total Fake Traffic, Finance, 2022



Fake Traffic Across Industries

Gambling and Gaming

Far-and-away the highest fake traffic rate of any industry evaluated in this report was that of the Gambling and Gaming industry, which has the difficult distinction of having a 49.1% total fake traffic rate, heavily weighted by a direct traffic fake traffic rate of 55.1%, versus organic and paid rates of 6.1% and 5.7%, respectively. The vast majority (89.9%) of those fake visits came through click hijacking attacks.

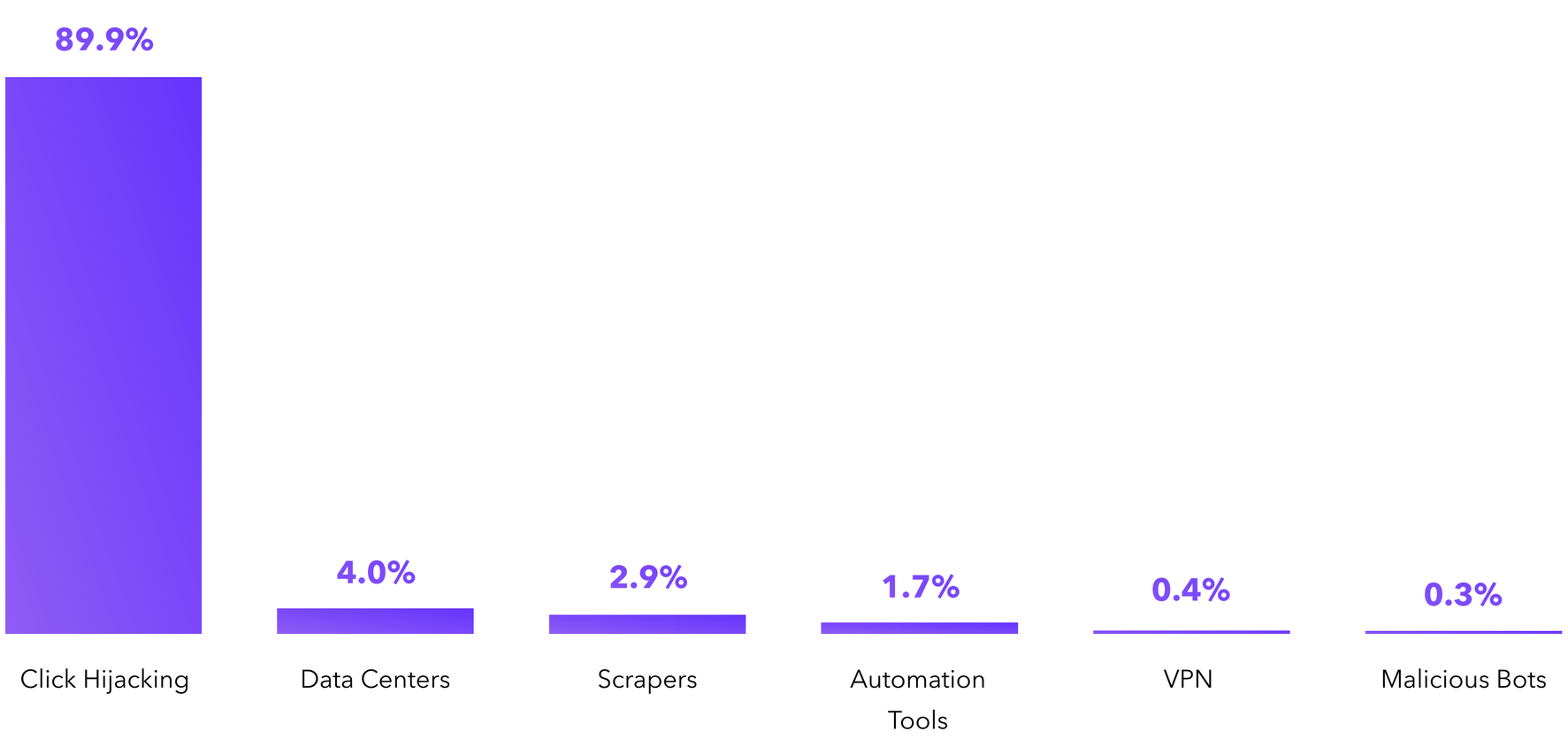
49.1%
Overall

5.7%
Paid

55.1%
Direct

6.1%
Organic

Threat Types as a Percentage of Total Fake Traffic, Gambling and Gaming, 2022



Fake Traffic Across Industries

Healthcare

The United States Department of Health and Human Services Office for Civil Rights reported that 594 data breaches took place between Jan. 1 and Oct. 31 of 2022 , with an average of 60 data breaches being reported each month. Often, hackers gain entry to networks through unsecured connected devices, but often the first point of contact was the target's website.

In 2022, healthcare websites had an fake traffic rate of 11.6%, and a majority of that bad traffic was comprised of scrapers (45.1%), which can potentially trawl a website for vulnerabilities or unsecured data.

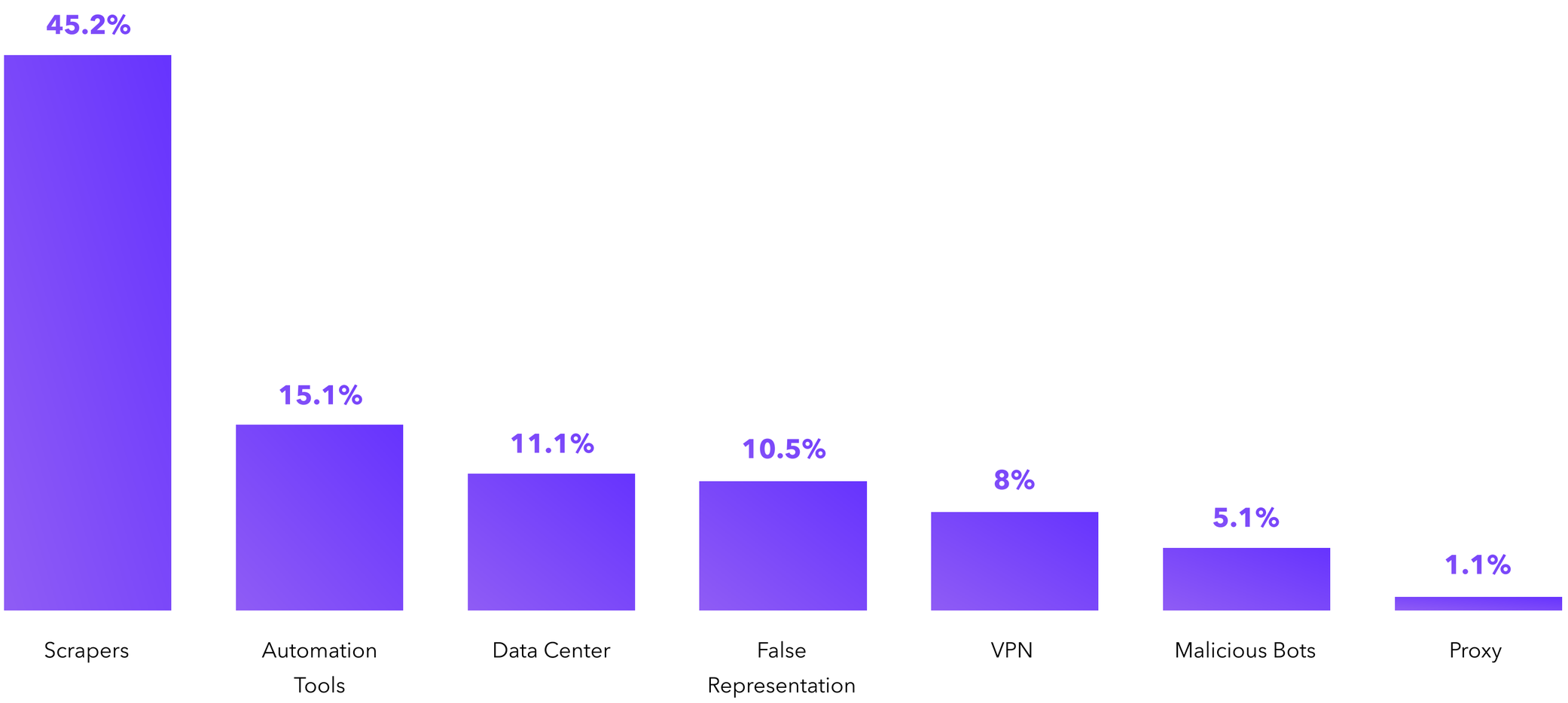
11.6%
Overall

2.5%
Paid

21%
Direct

13.8%
Organic

Threat Types as a Percentage of Total Fake Traffic, Healthcare, 2022



Fake Traffic Across Industries

Insurance

Like the healthcare industry, insurance companies, if breached, represent a treasure trove of valuable PII for hackers. And, like Healthcare, Insurance companies are a favorite target of web scrapers searching for vulnerable or unsecured data. In 2022, 13.7% of all traffic to insurance websites was invalid, and over two-thirds (67.8%) of that fake traffic was web scrapers.

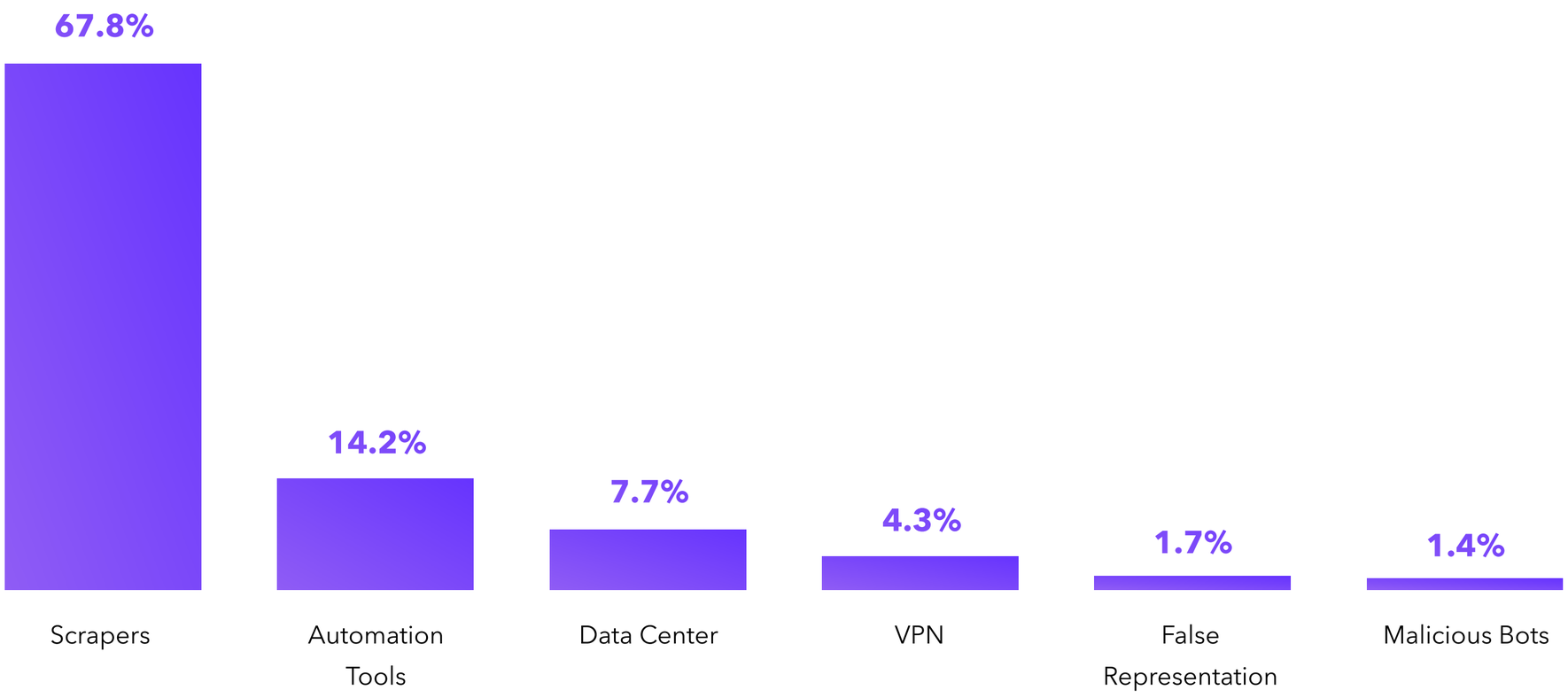
13.7%
Overall

2.4%
Paid

32.2%
Direct

2.5%
Organic

Threat Types as a Percentage of Total Fake Traffic, Insurance, 2022



Fake Traffic Across Industries

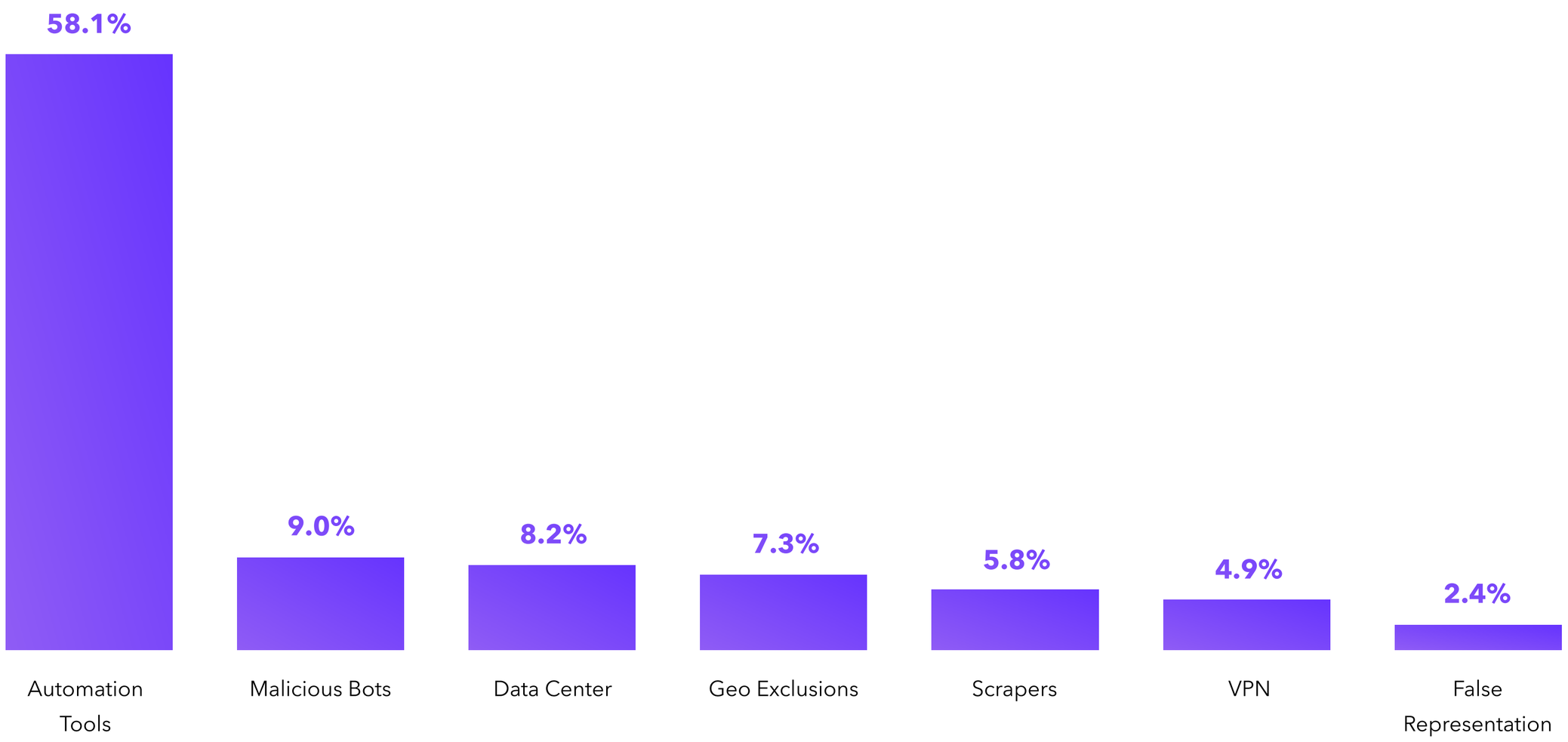
Retail

Between price scrapers, checkout bots, scalper bots, and card skimming attacks, there are a lot of threats tailored specifically to defrauding or otherwise targeting retail and eCommerce businesses

and that helps to explain why 16.4% of all traffic to retail sites was fake in 2022. Of that fake traffic, known malicious bots made up 9%, or approximately 1.5% of all traffic.

16.4%	3.0%	34.5%	4.4%
Overall	**Paid**	**Direct**	**Organic**

Threat Types as a Percentage of Total Fake Traffic, Retail, 2022



Fake Traffic Across Industries

Telecommunications

Telecom providers are a popular target for Distributed Denial of Service (DDoS) attacks, which attempt to disable a target website by flooding it with a massive volume of fake traffic in order to overwhelm and disable network infrastructure. These attacks are almost always carried out by botnets, large networks of connected devices (which could be user devices or simple IoT devices) infected and controlled by bots. In 2022, Telecommunication and Internet Service Provider websites had an overall fake traffic rate of 17.3%.

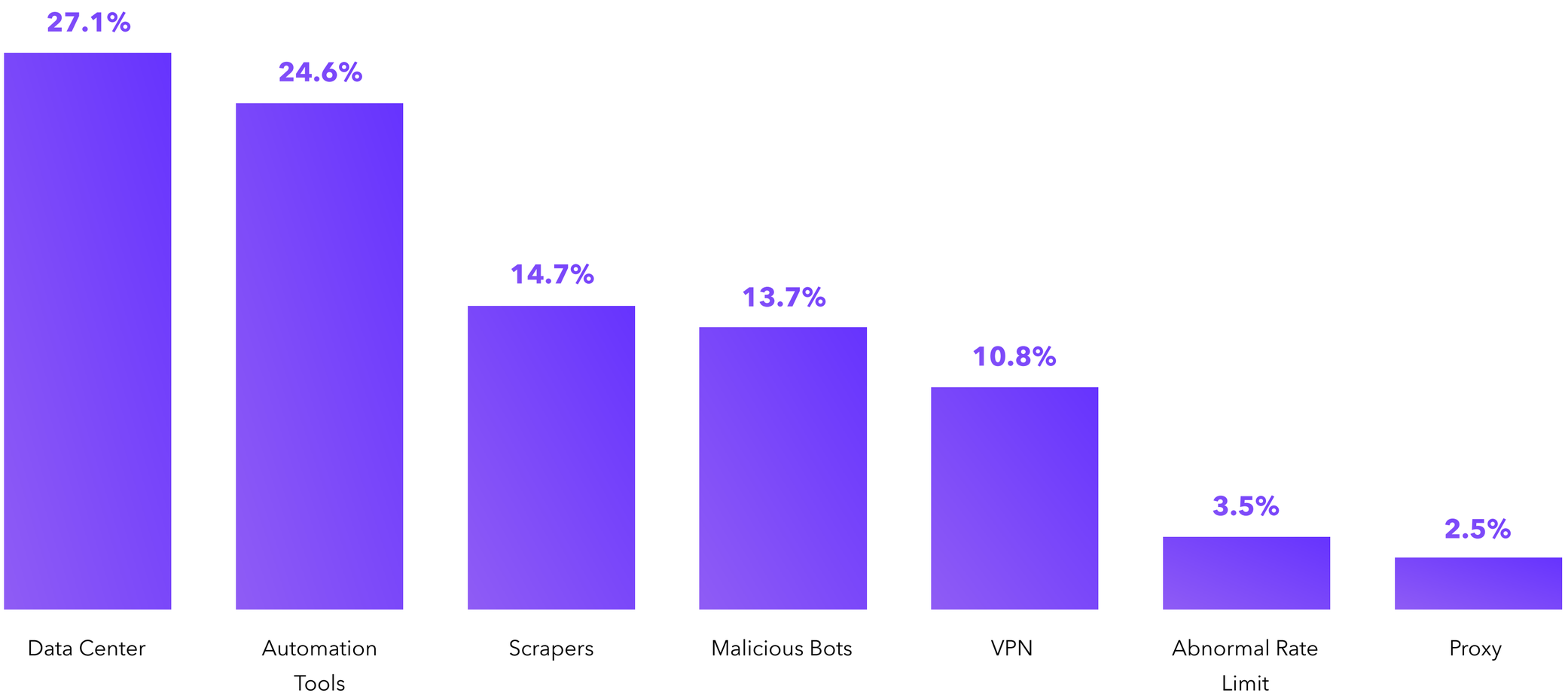
17.3%
Overall

7.1%
Paid

24.3%
Direct

9.6%
Organic

Threat Types as a Percentage of Total Fake Traffic, Telecommunications, 2022



Fake Traffic Across Industries

Travel & Hospitality

Travel and hospitality businesses faced a lower than average invalid rate in 2022 with 4.7% of overall traffic comprised of invalid traffic. However, these industries faced increasing traffic from specialized web scrapers, which represented 30% of all fake traffic attempting to interact with travel and hospitality pages.

The majority of this traffic is likely due to price scrapers from competitors and price comparison sites, although illicit web scrapers have also been leveraged to extract personal information, such as email addresses or credit card numbers, which can be used for nefarious purposes such as spamming, identity theft, or fraud.

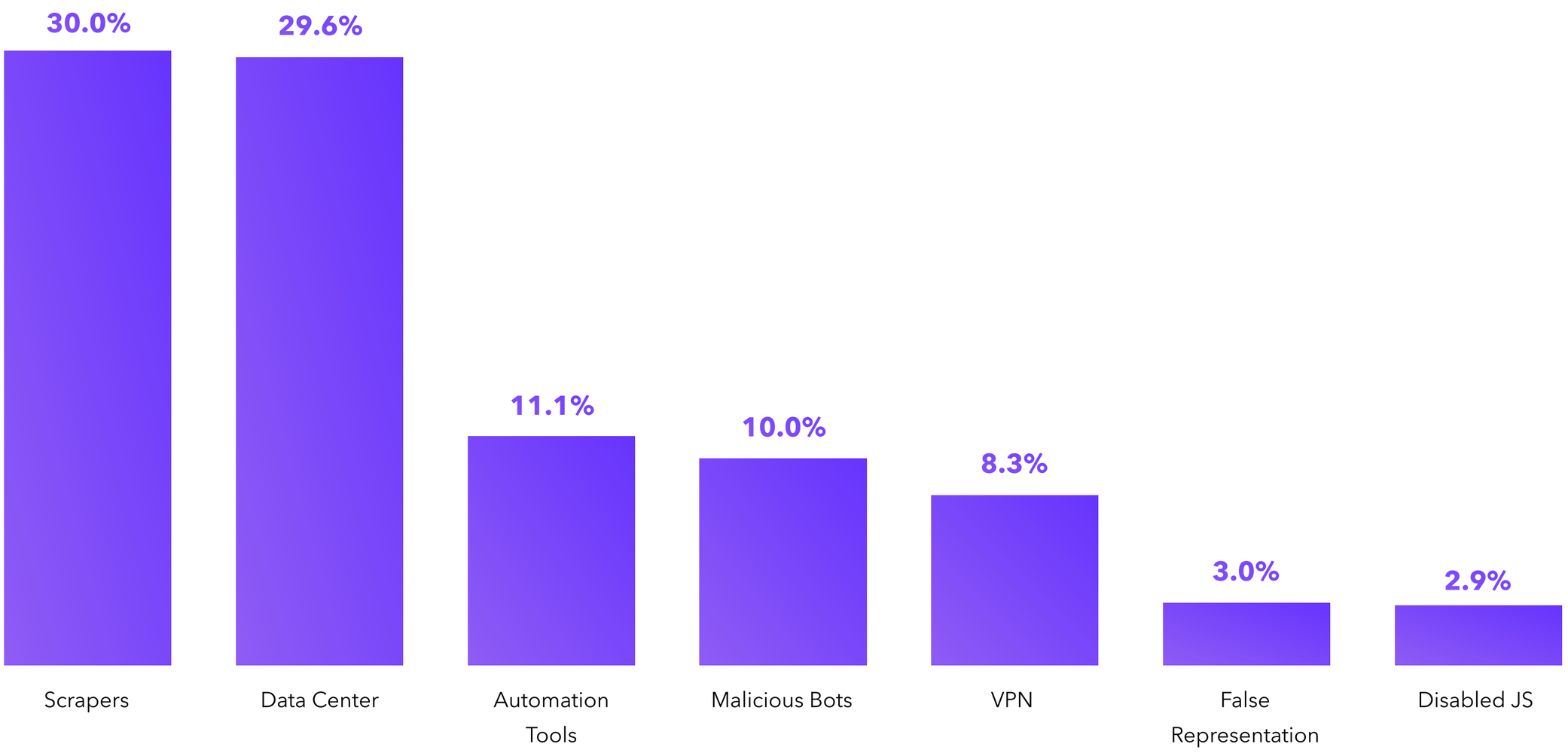
8.7%
Overall

3.3%
Paid

14.4%
Direct

3.0%
Organic

Threat Types as a Percentage of Total Fake Traffic, Travel and Hospitality, 2022



Fake Traffic Across Industries

Manufacturing

The manufacturing industry is not typically as ‘consumer-facing’ as other industries covered in this report, and as such, manufacturing websites typically attract a lower volume of traffic, and may be treated as somewhat of an afterthought. But fake traffic affects every corner of the internet, and manufacturing domains are no exception.

In 2022, 12.7% of all traffic to manufacturing websites was fake. A large portion of this traffic was made up by automation tools, web scrapers, and browsers running with disabled JavaScript (typical of headless browsers). This suggests a higher-than-average rate of attempts to find and exfiltrate data from manufacturing domains.

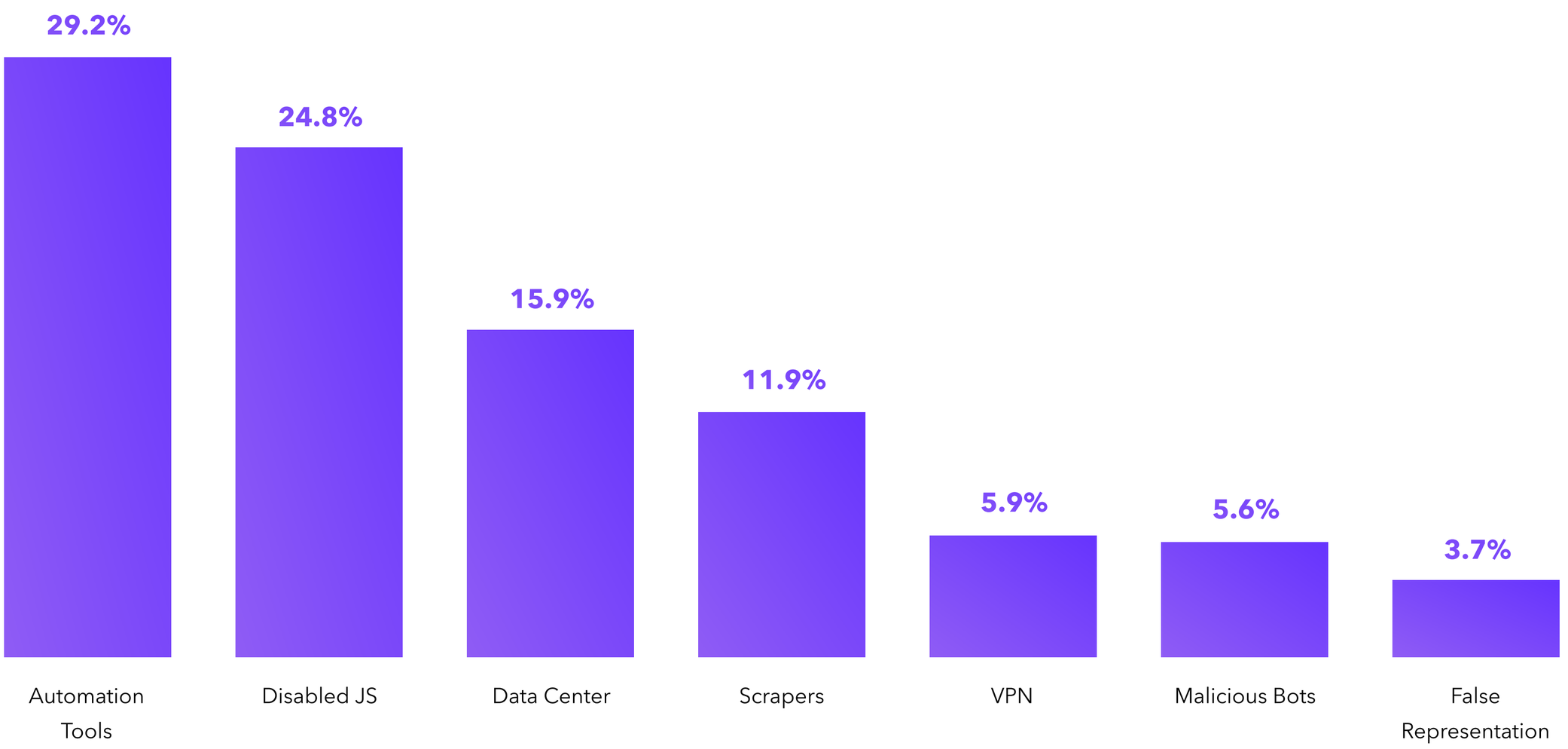
12.7%
Overall

3.0%
Paid

32.4%
Direct

4.4%
Organic

Threat Types as a Percentage of Total Fake Traffic, Manufacturing, 2022



Fake Traffic Source by Region

We evaluated the volume of invalid traffic originating from four different regions: North America, EMEA, APAC, and LATAM. By analyzing the amount of IVT from each of these regions, we can gain insights into the prevalence of fraudulent activity in each market and identify potential factors that may contribute to higher levels of invalid traffic. It's important to note that these statistics represent the invalid traffic *originating* from each region, and not where that traffic ends up.

Threat Types as Percentage of Total Fake Traffic, 2022

17.0%
North America

18.9%
EMEA

18.1%
APAC

8.7%
LATAM

Fake Traffic Source by Region

North America

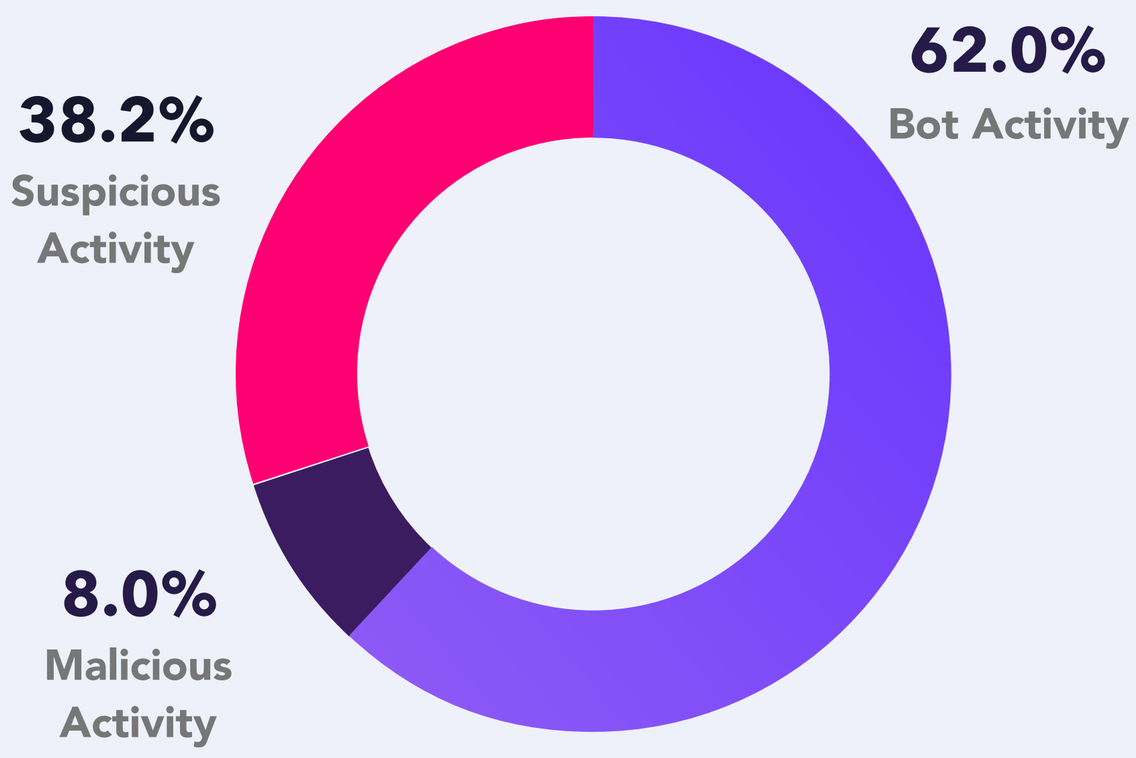
In 2022, fake traffic made up **17.0%** of all traffic originating from North America, with that fake traffic largely comprised of bot activity, specifically automation tools and scraper bots.

North America, specifically the United States where we tracked an average fake traffic rate of **25.3%**, is known for being one of the largest technology hubs in the world. With a strong presence of major tech companies, it is also home to a large number of digital advertising companies and marketers who use automation tools and web scrapers to boost their online presence.

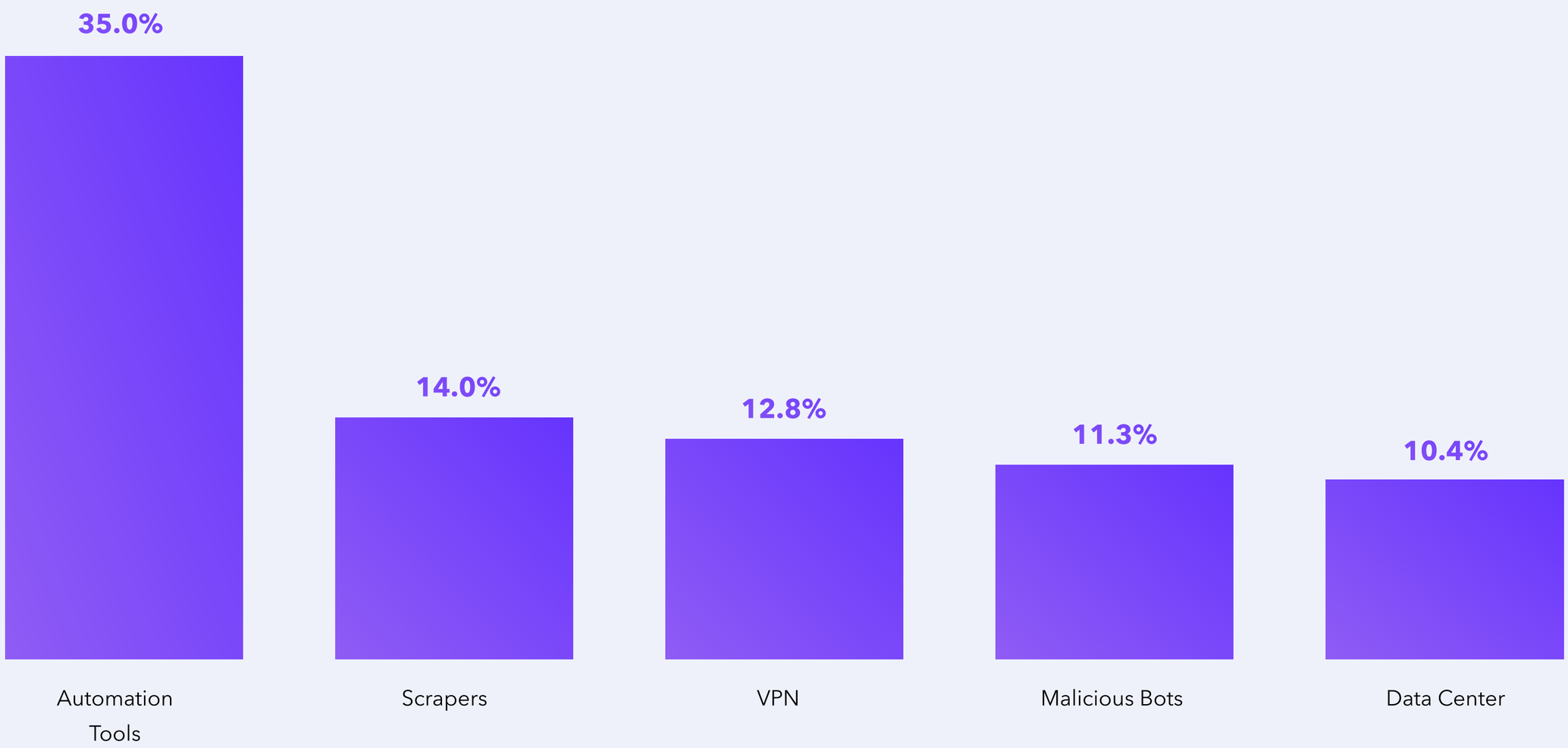
17.0%

Fake Traffic Rate

Fake Traffic Composition, North America, 2022



Threat Types as Percentage of Total Fake Traffic, North America, 2022



Fake Traffic Source by Region

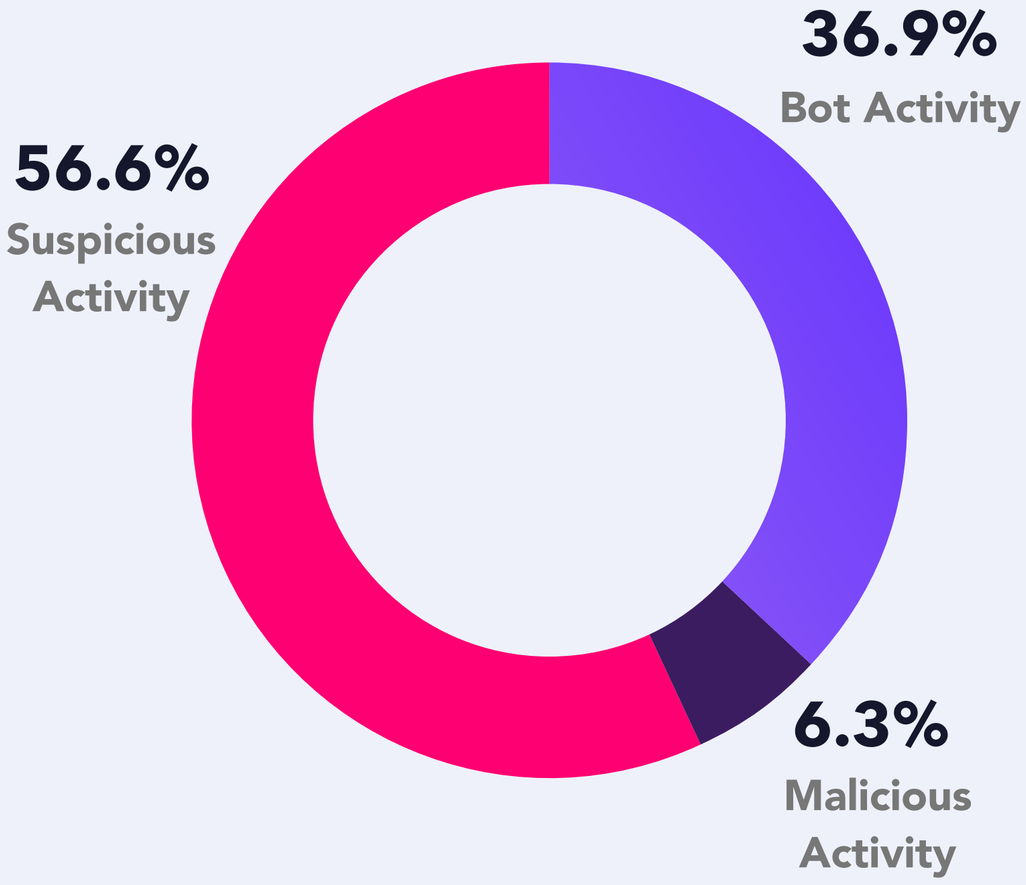
EMEA

In 2022, **18.9%** of all traffic originating in EMEA was invalid, the highest average fake traffic rate of any region. That fake traffic largely consisted of suspicious activity, such as VPNs which may be used to hide user identity or simply to bypass regional browsing restrictions. Click hijacking and malicious bot attacks also represented a significantly higher than average amount of traffic. This broad region contains the two top contributing nations to fake traffic world-wide: Nigeria and Greece, which had total fake traffic rates of **77.3%** and **48.5%**, respectively.

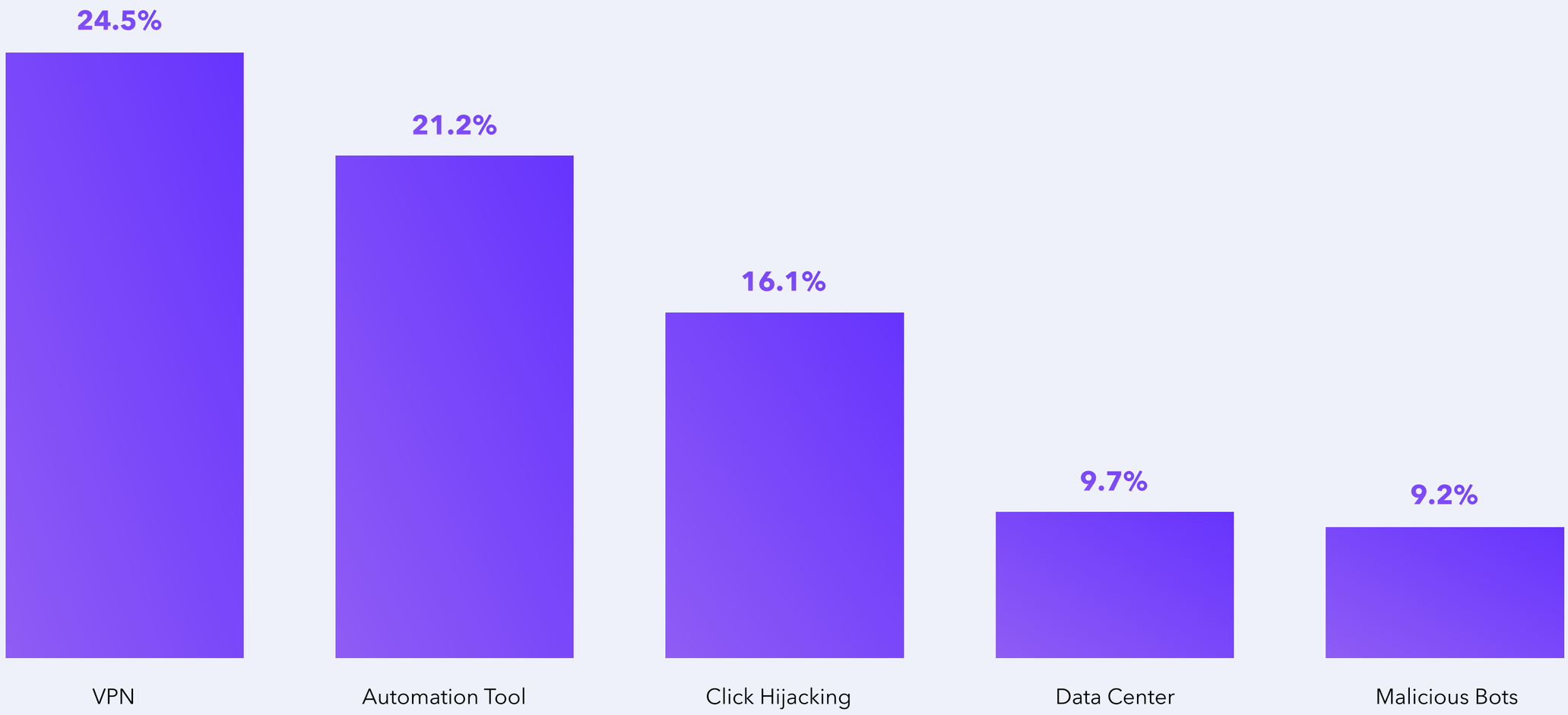
18.9%

Fake Traffic Rate

Fake Traffic Composition, EMEA, 2022



Threat Types as Percentage of Total Fake Traffic, EMEA, 2022



Fake Traffic Source by Region

APAC

Originating from the APAC region, fake traffic made up **18.1%** of all traffic in 2022.

Significantly, that fake traffic had the largest composition of malicious traffic of any region, at **37.0%.**

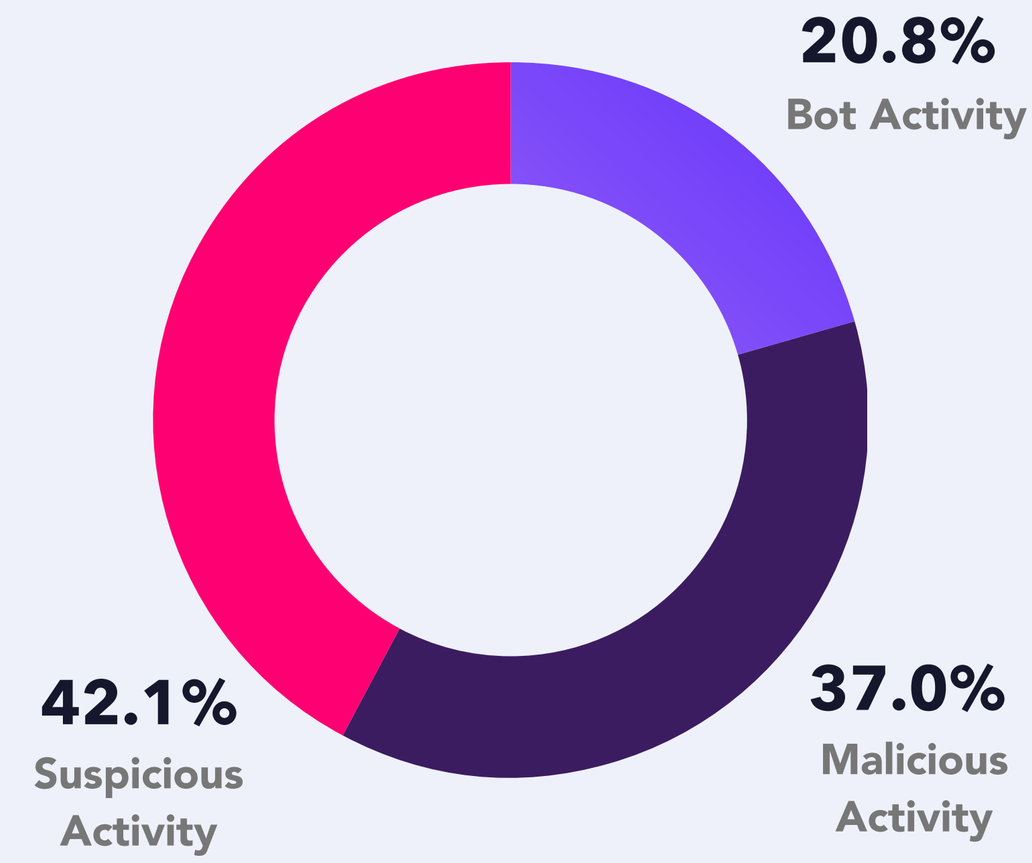
The largest contributing threat types were Disabled JavaScript, at 35.4% of all fake traffic, and Click Hijacking, at 31.4%.

APAC, particularly, China, the Philippines, and Indonesia, is known as a global hub for click farm businesses, where businesses hired by the highest bidder drive clicks and fake traffic to generate ad revenue or engagement for fraudsters.

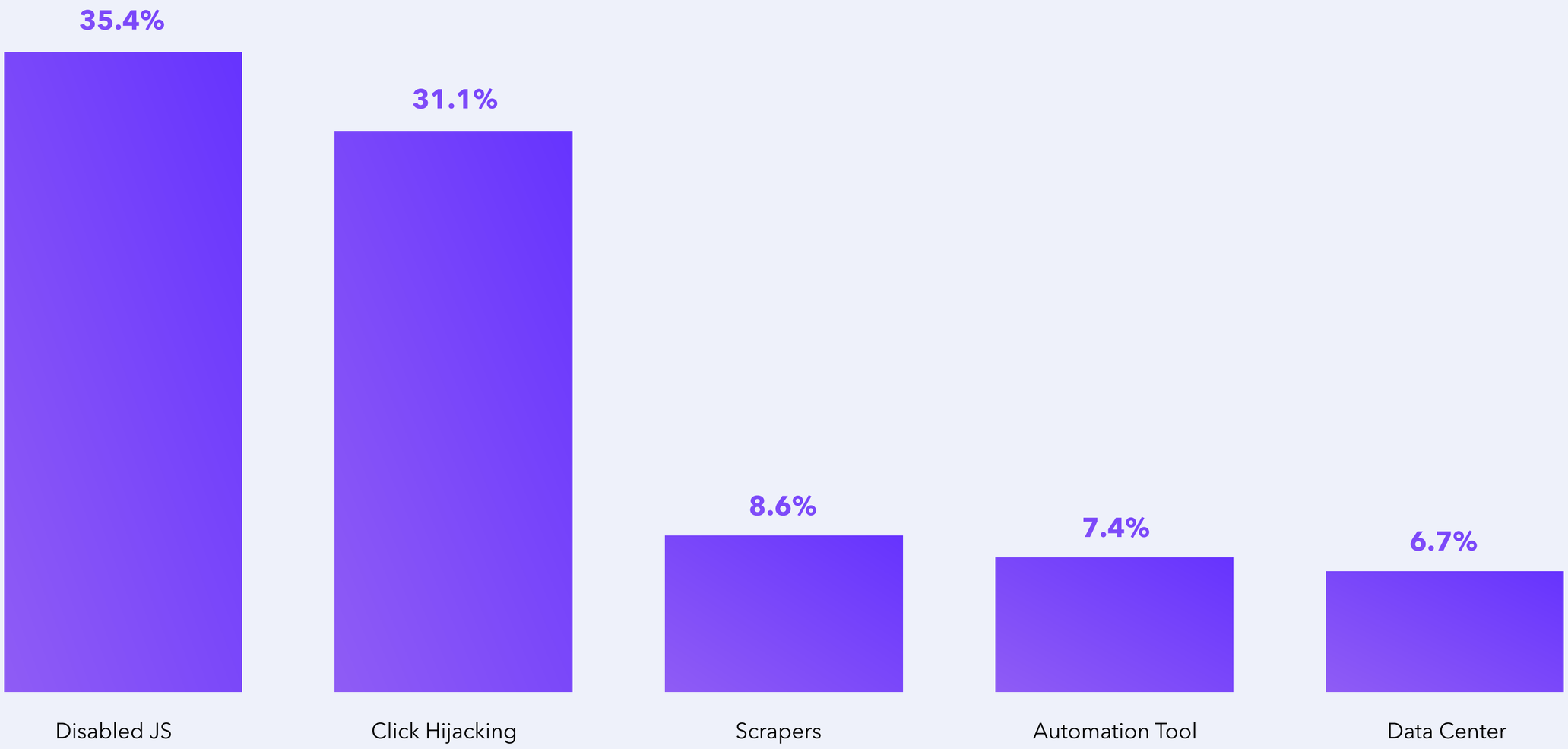
18.1%

Fake Traffic Rate

Fake Traffic Composition, APAC, 2022



Threat Types as Percentage of Total Fake Traffic, APAC, 2022



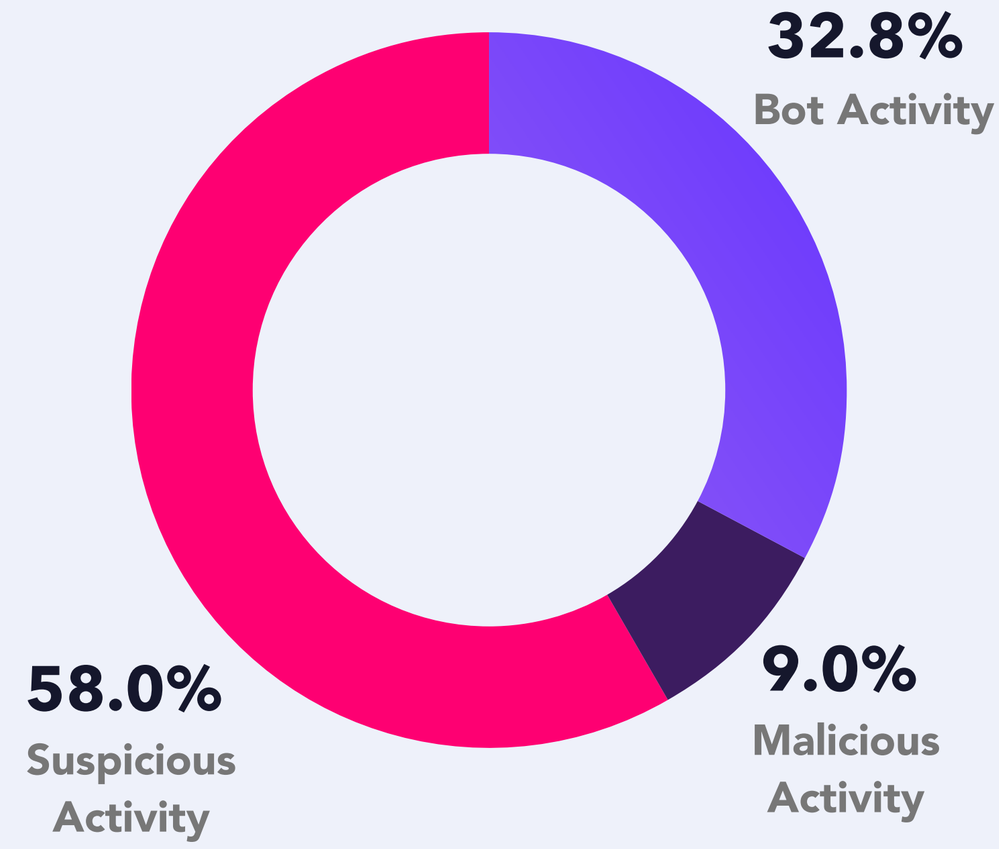
Fake Traffic Source by Region

LATAM

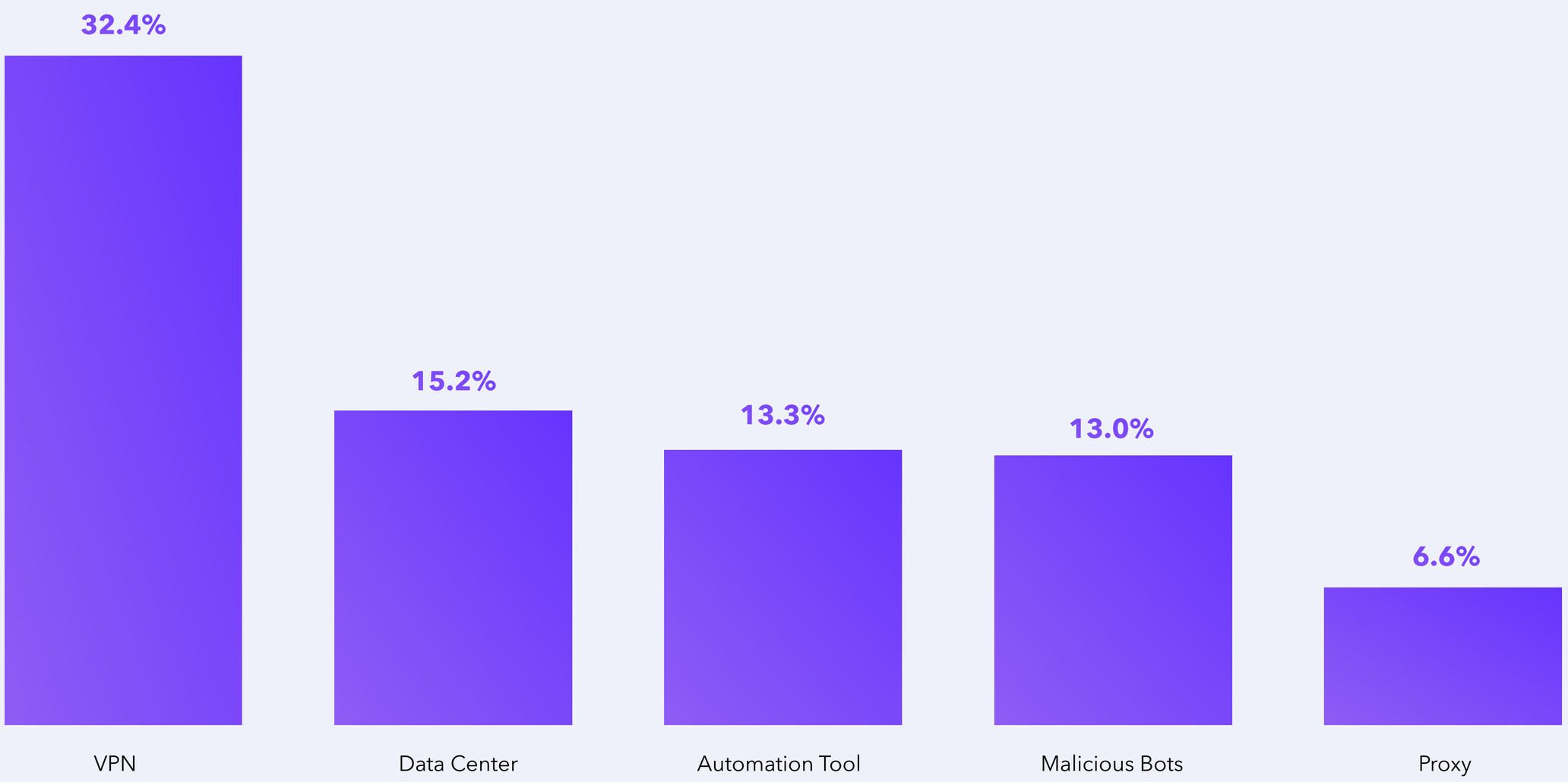
At 8.7% of all traffic in 2022, the LATAM region generated the least fake traffic rate of all regions worldwide by a wide margin. The majority of the fake traffic we tracked from LATAM consisted of VPNs and proxy tools, which made up a combined 49% of fake traffic from the region. This could be symptomatic of fraud in the region, but may also represent users attempting to bypass censorship or regional restrictions. It's not all good news, though. At 13.0%, malicious bots made up a larger percent of fake traffic in LATAM than in any other region.

8.7%
Fake Traffic Rate

Fake Traffic Composition, LATAM, 2022



Threat Types as Percentage of Total Fake Traffic, LATAM, 2022



The Business Impact of Fake Traffic

Businesses need every dollar they spend to yield a good return. Fake traffic like bots, automation tools, fraudulent accounts, and click farms stand in direct opposition to that goal. In 2022, global spending on digital advertising surpassed $600 billion USD, according to Statista.com. By applying our average invalid rate for paid traffic to that number, we are able to conservatively estimate that approximately $35.7 billion of ad spend was wasted on fake and fraudulent traffic in 2022.

Beyond advertising budgets, fake traffic also destroys potential revenue opportunities. Return on ad spend (ROAS) is a metric that measures the effectiveness of an advertising campaign by calculating the return on investment (ROI) generated by the ad spend. The formula is simple: for every dollar spent on advertising (X), businesses can expect 1.5X, 2X, or 4X in return.

According to Adadaco, the average ROAS for eCommerce businesses is 4:1–meaning that businesses lost $142.8 billion dollars in potential revenue to fraudulent traffic in 2022.

It should be noted that these lost revenue opportunities do not account for additional damages caused to the paid marketing apparatus, including pollution of remarketing efforts and lookalike audiences, and skewing of automated optimization algorithms, which can cause even more revenue loss down the funnel.

Business Impact

Downstream Effects: Lost Efficiency, Skewed Analytics, Eroded Trust

In an increasingly KPI-driven marketing world, efficiency is paramount.

Marketers need to improve customer acquisition cost, lower cost per action, increase ROAS, increase contract value and shorten deal cycles. To do this, marketers must constantly experiment and analyze results. More data scientist than Don Draper, A/B testing, messaging changes, targeting parameters, and segmented audiences are the tools of the modern marketer. But without good data, none of those tools can function properly. The presence of bots and fake users in the marketing funnel undermines the very foundation that digital marketing is built on.
The old adage of “garbage in, garbage out” is applicable here.

When a marketer’s analytics is showing them 2 million unique monthly site visits, but they’re unaware that 25% of that is fake traffic, then forecasting, budget planning, A/B testing, optimization and measurement are all compromised.

Eroding Trust

Marketing programs succeed when they achieve a high degree of trust and transparency within their organization. When the sales team trusts the marketing team to deliver quality leads, when management can rely on marketing forecasts to be accurate and when marketers themselves can rely on the numbers they’re looking at to be true, then they’re in a position to win.

But allowing fake traffic into their funnels undermines all of the above. If inbound leads are coming from fake users, the relationship between sales and marketing suffers.

A recent study by ZoomInfo found that sales and marketing departments lose approximately 550 hours and as much as $32,000 per sales rep from using bad data, much of which is a direct result of fake leads in their CRM.

Business Impact

Twitter, PayPal, and The Fake Web as a Threat to Brand Reputation

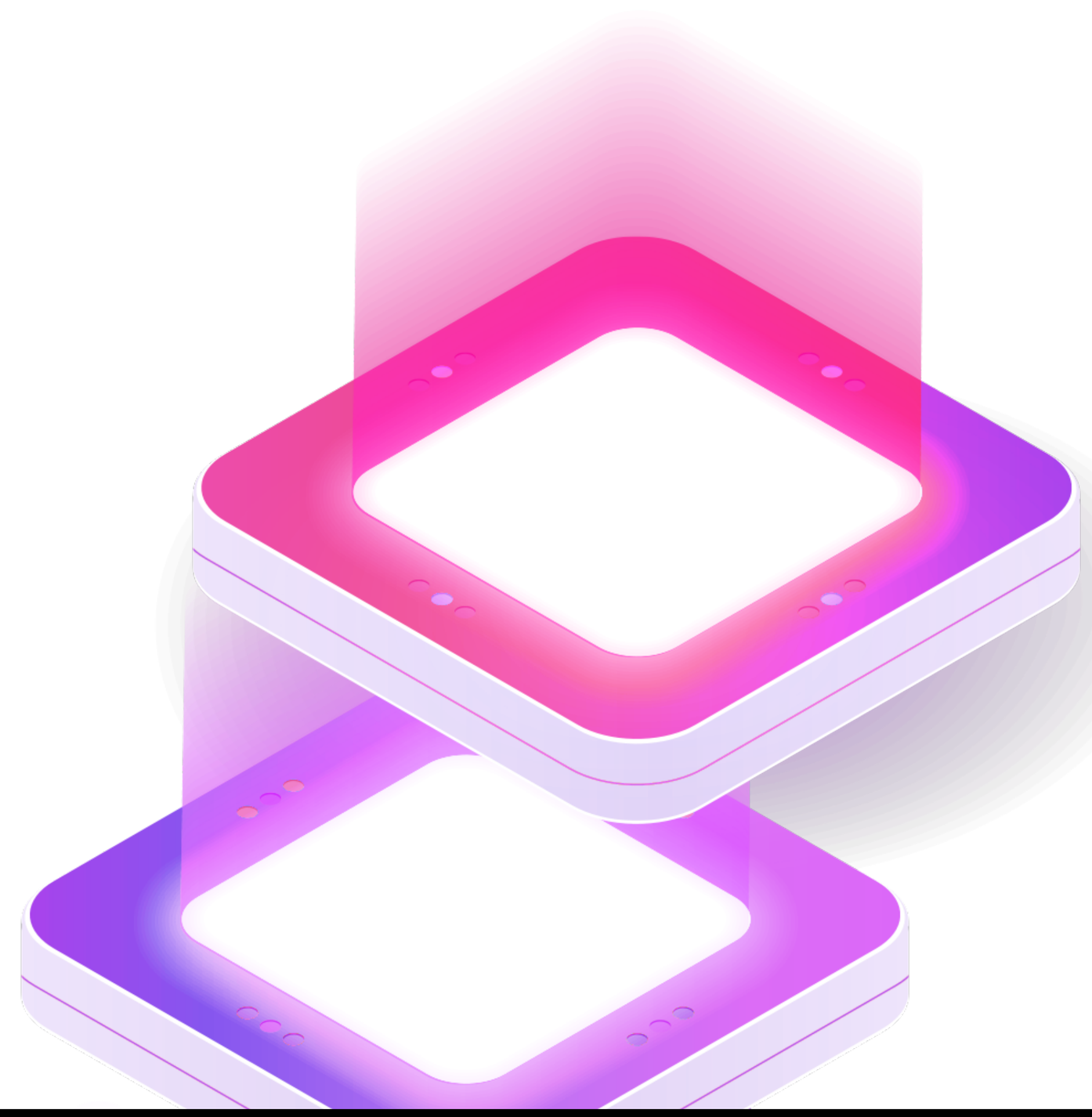
Beyond simply damaging interorganizational trust, fake traffic can create significant reputational risks for brands and businesses. Consider the Twitter debacle concerning fake bots: how many eager buyers do you think are lining up to buy ads on a platform with a notorious bot problem?

And Twitter isn't the only victim of the "Fake Web." In February 2022, Elon Musk's alma mater PayPal discovered approximately 4.5 million fake users on its payment processing platform program. These 'users' were exploiting the company's sign-up incentives, which offered users $5 or $10 bonuses, at a massive scale.

But that fraud was the least of PayPal's worries. When shareholders found out about the failures in the company's customer acquisition strategy and the accuracy of its user-growth reporting, stock fell sharply--down 25% in just 24-hours.

These issues are not merely inconvenient; they erode trust between consumers and the brands they choose to do business with. When trust is broken, consumers may choose to buy from competitors instead or avoid making similar purchases or using similar services in the future.

Ultimately, the "Fake Web" isn't going anywhere, and as legislators and the public become more aware of the issue we can expect no shortage of similar stories in 2023.



Looking Forward: How Fake Traffic Will Change in 2023 and Beyond

From 2021 to 2022, we tracked a 163% increase in the total number of invalid interactions with client properties.

In 2023, the trend of increasing fake traffic is likely to continue, largely driven by rapid breakthroughs in AI technology that have the potential to both lower the barrier to entry for creating botnets, and exponentially increase the sophistication and capability of malicious bots.

AI Advances Lead to Increased Bot Activity

The development of advanced AI models such as ChatGPT and their increasing accessibility have made it easier for individuals to create and use bots for malicious purposes. These bots can be used to scrape websites, fill out forms, and generate false or misleading traffic. Currently, ChatGPT will generate a simple web scraping bot on request, though the code is typically inaccurate and the bots rarely work. However, OpenAI, the creator of ChatGPT and the underlying AI model that it runs on, has announced plans to release GPT4, the next iteration of the model, this summer. Details on GPT4 are sparse, but given the rapid advances from GPT3 to 3.5 alone, we can expect much improved capabilities.

Increased Bot Sophistication

Cybersecurity is a game of cat and mouse. As defenses improve, so too will bots and attackers in their attempts to overcome them. However, the advent of powerful, free-to-use AI models has the potential to upend that paradigm and hand bad actors a leg up.

For example, bots may be able to leverage AI to generate convincing content, such as misleading reviews, comments or user-generated content, convincing phishing emails, or even fake chatbots at a scale far-beyond current capabilities.

These increased capabilities have the potential to create a challenge that can only be overcome with a concerted and multi-faceted effort. The old ways of manually blocking IPs and leveraging Google blocklists limited to 500 simply will not scale. The modern business needs to monitor incoming traffic and automatically block and detect fake traffic before it gets into their funnel.

About CHEQ

CHEQ is the leader in Go-to-Market Security, trusted by over 15,000 customers worldwide to protect their metrics, marketing efforts, and customer data from those with potentially malicious intent online.

Powered by award-winning cybersecurity technology, CHEQ offers the broadest suite of solutions for securing the entire GTM org from threats to business continuity, brand reputation, and marketing effectiveness.

Schedule a free trial today to learn how CHEQ can help you block fake traffic on your website and keep your go-to-market operation clear of bad leads and malicious actors.