The State of Fake Traffic:
Financial Services

CHEQ

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 for financial services and financial tech.

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 legitimate customers. This could mean harmless bots like a search engine's crawlers, or malicious traffic like ad fraud botnets. Research has revealed that upward 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 financial institutions and their customers.

For finance marketers, fake traffic is a concern because it can cause credential stuffing attacks on loyalty programs, new account fraud from stolen data, promotion abuse and exploitation, and other serious business threats. Thus, we should look at the effects of the "Fake Web" as a strategic business issue and a brand safety concern that extends far beyond the marketing department.

In many instances, entire organizations 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 financial businesses operating today in this era of fake traffic.

*Wired.com, 2022

Taking a Look at the Data

Following several infamous data breaches 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. Scrapers, specifically, can cause a plethora of problems including extracting personal data and hacking into confidential systems.

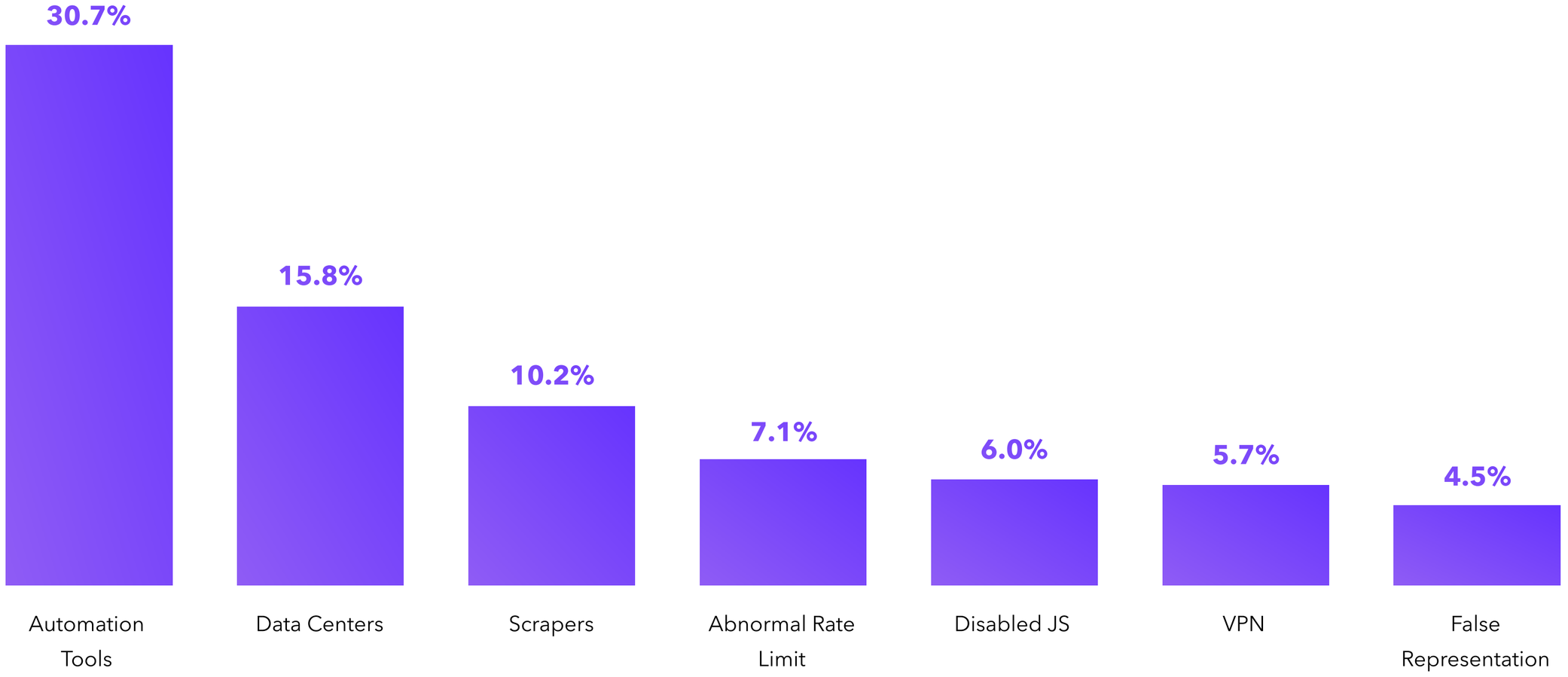
13%
Overall

3.1%
Paid

19.7%
Direct

4.9%
Organic

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



What This Means for 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, sources of truth become unreliable, privileged information becomes hack-able, and brand safety and reputation are largely at risk.

When customers cannot trust your organization, or they have negative associations with your brand, growth and business continuity become increasingly difficult to maintain.

That's why it is important for us to convey just how widespread and pervasive the threat of fake traffic is. In the financial industry alone, fake traffic can cause a variety of strategic business problems including:

- Exploitation of promotions and discounts
- New account fraud
- Server overload and denial of services
- Skewed metrics and data

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

Case Study: A Fortune 50 Financial Institution & The Fake Web as a Threat to Operational Efficiency

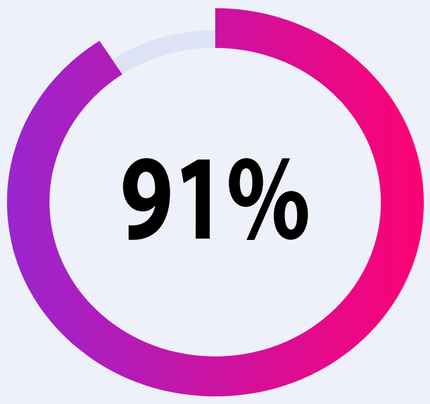
The Fake Web goes beyond causing mere inconveniences and reputational risks; when a go-to-market organization is not holistically protected, they can end up with major issues of operational efficiency. CHEQ worked with a Fortune 50 financial organization, who - prior to our partnership - was experiencing unexplained volatile website traffic patterns.

Through a careful analysis, we were able to determine that as much as 10% of their paid media traffic was being spent on bots and other invalid users, causing their key metrics to be unpredictable and large quantities of their advertising budgets to be wasted.

This led to significant monetary losses for the institution, which brought into question the overall effectiveness and efficiency of their marketing operation as a whole.

When the organization decided to act - by implementing go-to-market security measures and blocking invalid traffic - their results drastically improved. They experienced real-time visibility into how fake traffic was impacting their efforts, and consequently were able to reduce malicious bot traffic by 91%.

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 this coming year.



reduction in
malicious bot traffic

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.