

# Where Is Ad Fraud Coming From?

An In-Depth Look at Fraudulent Traffic Origins

May 2018 - July 2018





# The Discovery

When talking about the sources of ad fraud, there's a common narrative that all ad fraud originates from certain regions of the world. However, as fraudsters become more sophisticated, that myth is quickly being debunked.

The reality is ad fraud can take place from anywhere around the globe. Fraudsters aren't limited to one location of operations. They can conduct their fraud abroad with tactics like fraudulent cloud computing and domain spoofing, just to name a few.

Some attacks may be initiated by people or groups from different locations, while others are digitally enacted from locations that aren't spoofed or faked. However, when correctly identified, many attacks (more specifically the ones we are going to discuss in this report) come from data centers using sophisticated methods to hide their origins. These are popular due to the large volume of data centers around the globe. New and unknown data centers are constantly popping up, making it difficult for some companies to accurately identify data center traffic.

From **May 2018 through July 2018**, our ad fraud solution Anura® watched and recorded the growth of bad web traffic being monitored on behalf of our clients. For the purposes of this report, we focused on U.S. traffic and European traffic as these regions had the highest amount of overall fraudulent traffic growth during this time frame.

Based on a series of proprietary rule sets, Anura identified specific factors that caused certain sources of traffic to be marked as fraudulent. Anura found that one rule set in particular, User Environment, triggered the majority of bad traffic rulings. Curious for the sudden spike in fraudulent traffic, we decided to dive down to the granular level to see what was causing the growth.

47.06%

Percentage of Bad  
Traffic Worldwide

47.67%

Average Percentage  
of Bad U.S. Traffic

39.61%

Average Percentage of  
Bad European Traffic

## Applicable Rule Sets

To make accurate judgments on website visitor quality, Anura has a series of rule sets that powers the decision-making process. Each rule set is comprised of multiple formulas that work together to validate or invalidate every website visitor.

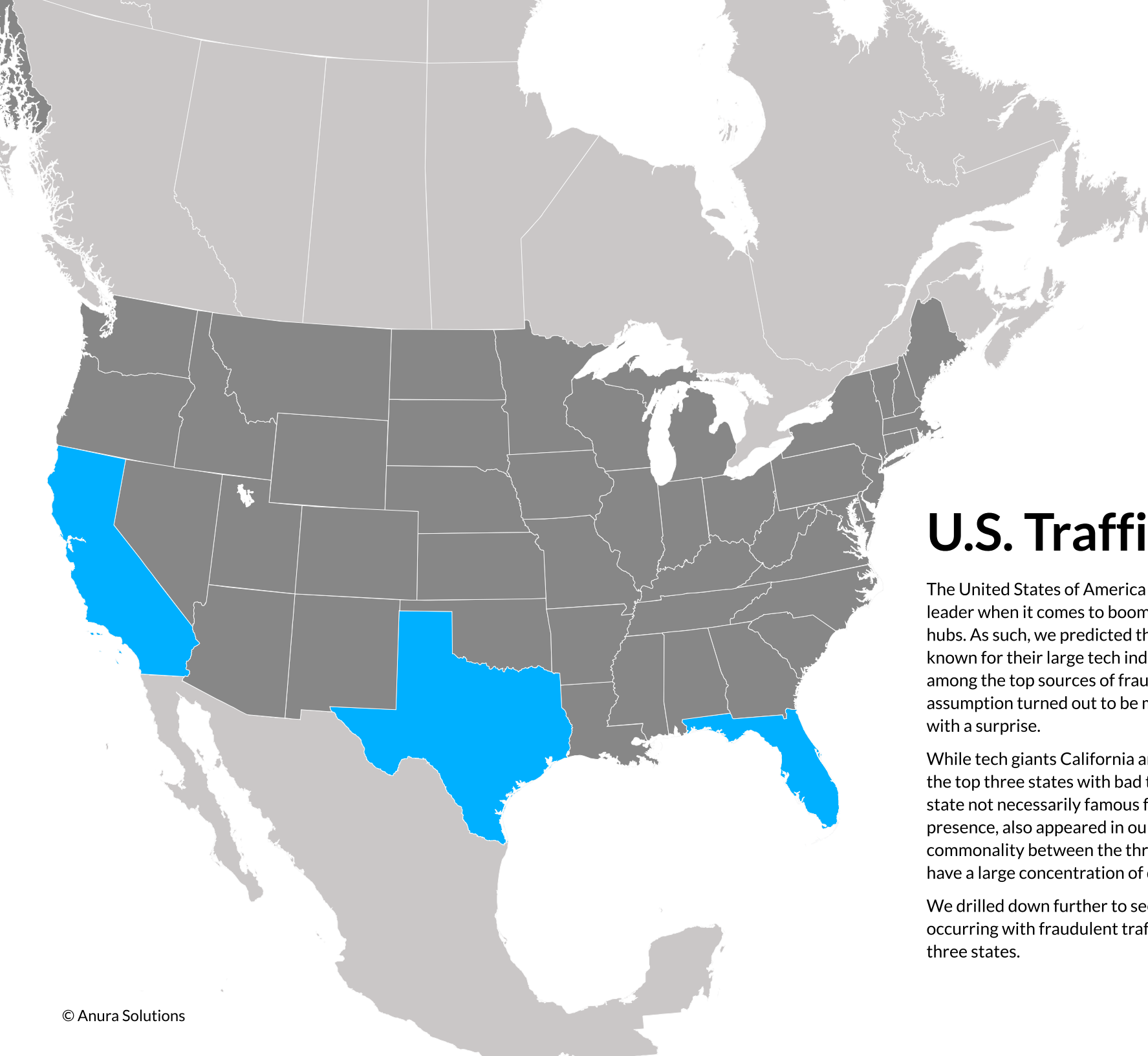
**User Environment.** This rule set analyzes and identifies abnormalities within a visitor's device or browser being used to interact with the web. It takes a top level look at several factors, including browser types, browser versions, and device types.

More sophisticated attacks come from User Environment. Fraudsters manipulate aspects of their user environments, making it seem like real users are coming from a variety of locations, devices, and browsers. Anura excels at catching more sophisticated attacks than other solutions, since Anura focuses on the user instead of vanity metrics.

**Spoofing.** This rule set is designed to validate whether a visitor is genuine or spoofed. Spoofing refers to the practice of masking aspects of a visitor's identity in order to deceive or trick another computer. Fraudsters use spoofed traffic to make it seem like visitors are coming from a variety of locations, when in reality, the traffic is probably coming from a single source.

**Traffic Origin.** The flow of visitors across the internet generates data which tells us where the visitor has been prior to visiting your website. With the information gathered, Anura reviews prior origin data to determine if it has come from a known fraudulent site, or if it gives indications of questionable origination.

**Data Center.** A data center is a facility that houses remote storage of data, web servers, and servers. While data centers are paramount in most networks' critical systems and are vital to daily operations, they do not typically generate website visitors. Anura routinely checks and verifies using in-house methods to ensure the visitor is not coming from a data center.



## U.S. Traffic

The United States of America remains a global leader when it comes to booming technology hubs. As such, we predicted that U.S. states known for their large tech industries would be among the top sources of fraudulent traffic. Our assumption turned out to be mostly accurate, but with a surprise.

While tech giants California and Texas ranked in the top three states with bad traffic, Florida, a state not necessarily famous for its industry presence, also appeared in our data. The commonality between the three states: they each have a large concentration of data centers.

We drilled down further to see what was occurring with fraudulent traffic in each of the three states.

# California

As the home to some of the biggest companies in tech and one of the most populated states in the U.S., it wasn't surprising to see California claim a spot near the top of the list.

According to Anura's analysis, the amount of bad traffic originating from the Golden State gradually decreased month-over-month. In May, bad traffic accounted for **59%** of all traffic passing through the platform. By July, that number dropped to **42%**.

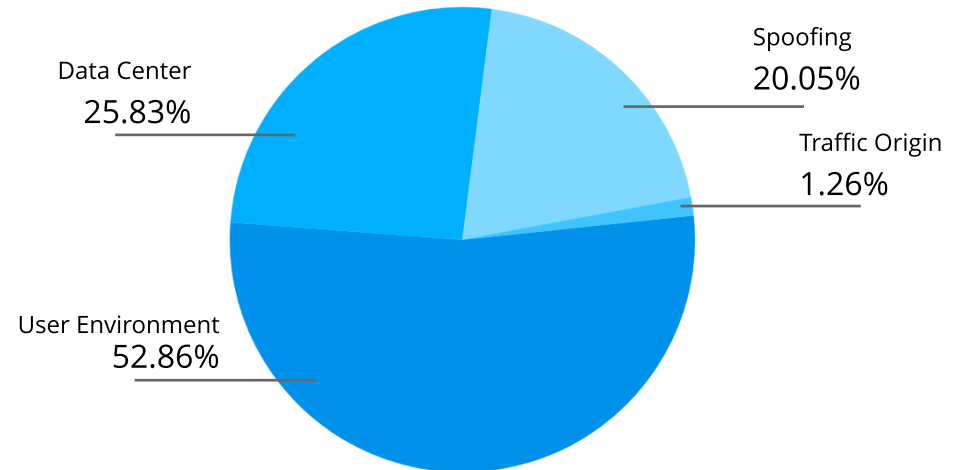
Approximately **52.86%** of the bad traffic coming from California triggered Anura's User Environment rule set. In fact, the number of instances in which this rule set was broken increased by **45%** from May to July. By comparison, data center traffic accounted for about **25.83%**.

California's top cities with the highest percentage of traffic included:

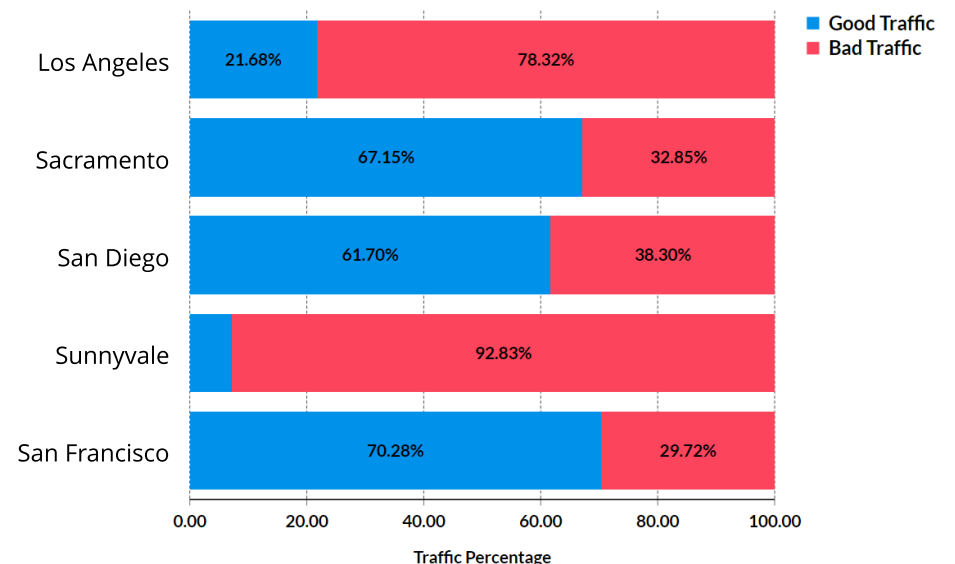
- Los Angeles
- Sacramento
- San Diego
- Sunnyvale
- San Francisco

Out of those five cities, Sunnyvale, a city considered part of Silicon Valley, had the highest amount of bad traffic. Anura determined **92.83%** of responses coming from this city were fraudulent. In addition, Anura's rule sets flagged a staggering **97.3%** as data center traffic.

California: Percentage of Rule Sets Broken



California: Top 5 City Rankings Based on Traffic





# Texas

Down in Texas, the tech industry is experiencing growth like never before, with major metropolitan areas like Dallas-Fort Worth and Austin being dubbed the Silicon Prairie and the Silicon Hills. Anura's data ranked Texas as the second worst state with bad web traffic, a number that increased **88%** by the end of the three-month study.

Like California, the overall percentage of bad traffic in Texas actually decreased from about **58%** in May to **36%** in July. However, bad traffic did spike in June at about **67%** for the month.

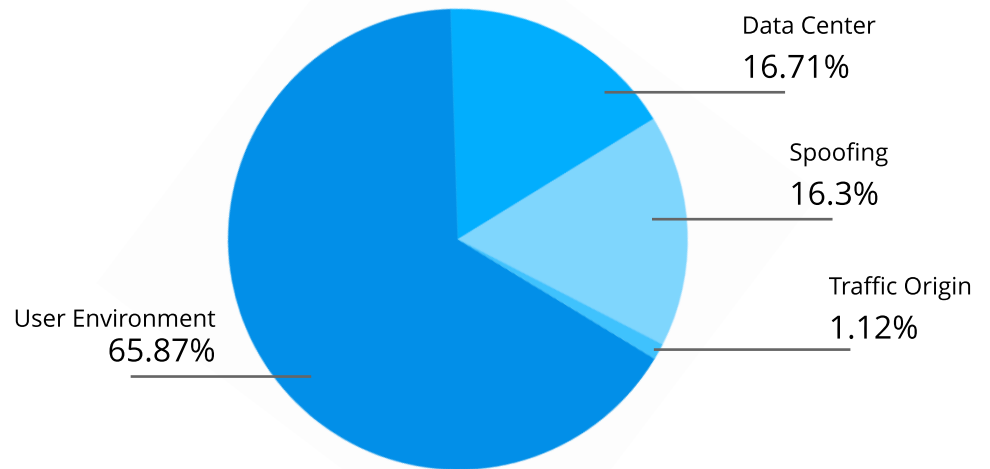
Anura found that **65.87%** of the bad traffic broke the User Environment rule set, a number that increased by **17%** over the three month period. Data center traffic was the second largest broken rule set, accounting for **16.17%** of bad traffic. Spoofed traffic followed closely behind at **16.3%**.

Texas's top cities with the highest percentage of traffic included:

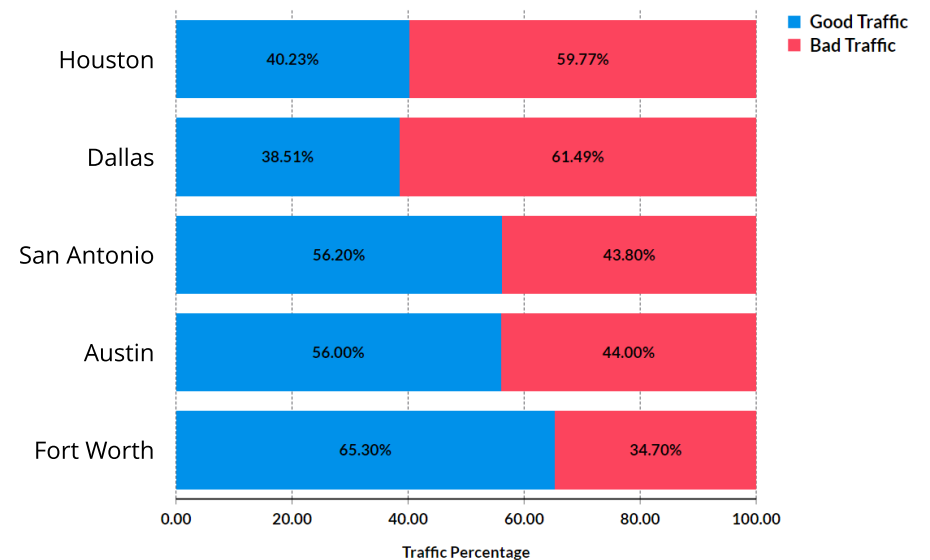
- Houston
- Dallas
- San Antonio
- Austin
- Fort Worth

Dallas slightly surpassed Houston by just **1.72%** for the city with the highest amount of bad traffic. Out of the **61.49%** of bad traffic coming from Dallas, **63.92%** identified as data center traffic, an interesting find considering Dallas is emerging as a top data center market in the U.S.<sup>1</sup>

Texas: Percentage of Rule Sets Broken



Texas: Top 5 City Rankings Based on Traffic



# Florida

Seeing Florida appear in the top results was unexpected, given the state nor any of its major cities aren't traditionally cited as key players in the U.S. tech industry.<sup>2</sup> Bad web traffic in Florida followed the same trend as Texas, with an overall decrease from **47.45%** in May to **30.64%** in July, but a sudden spike of **60.66%** in June.

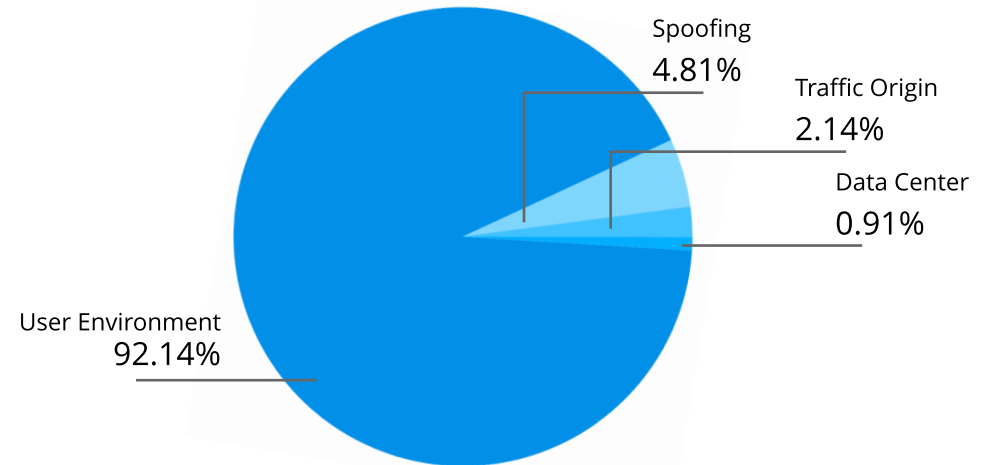
Like the other states, the User Environment rule set accounted for the majority of the bad traffic at **92.14%**, a number that increased by **63%** over the course of the study.

Florida's top cities with the highest amounts of traffic included:

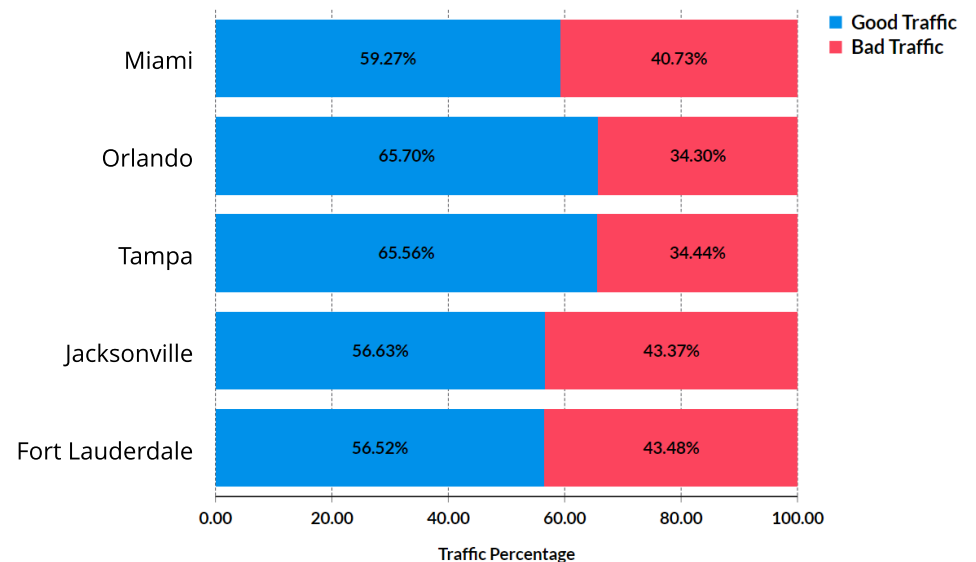
- Miami
- Orlando
- Tampa
- Jacksonville
- Fort Lauderdale

There weren't many significant differences in the amount of bad traffic coming from each city; however, Fort Lauderdale had the largest percentage of bad traffic at **43.48%**.

Florida: Percentage of Rule Sets Broken



Florida: Top 5 City Rankings Based on Traffic



# European Traffic

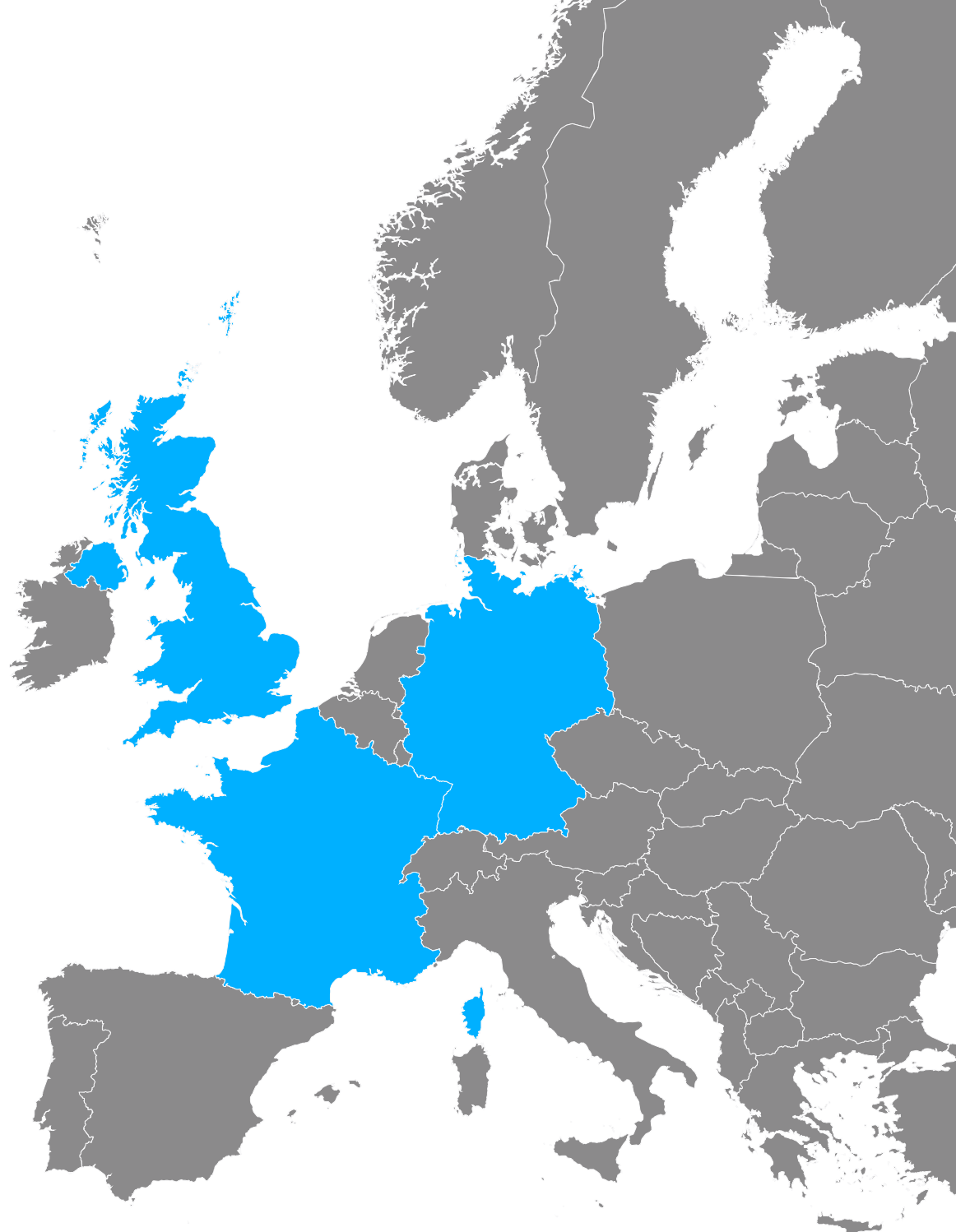
To see if fraudulent traffic was coming from areas that most presume generate dirty traffic, such as Russia, China, and India, we reviewed Anura's findings.

Surprisingly, our data showed that the traditional narrative was false. The biggest region of fraudulent traffic growth within that time period was Europe, with the percentage of bad web traffic rising by **51%** from May 2018 to July 2018.

Drilling down further, three European countries consistently appeared each month with noticeable growth in both traffic volume and the percentage of bad traffic. Those countries were Germany, France, and the United Kingdom. Mirroring the U.S., the commonality between these countries was the large data center market.<sup>3</sup>

Anura also showed mobile traffic for Germany, France, and the United Kingdom had increased by **4,864%** during the three-month period. Wondering why mobile traffic was growing, we did some research and discovered a trend in European mobile traffic growth. IAB Europe's June Report stated that **57%** of Europe's digital population uses both mobile devices and desktop computers to access online content.<sup>4</sup>

Meanwhile, studies conducted by IAB U.K. showed mobile devices account for **75%** of adults' time online.<sup>5</sup> These statistics align with the growth in traffic Anura recorded.



# Germany

Out of the three European countries, Germany's percentage of bad web traffic increased by **940%**.

In May, bad traffic passing through Anura was extremely low at just **6.63%**. That number increased to **27.48%** in June, then jumped to **68.94%** by July.

Analyzing Anura's rule sets, approximately **95.52%** of the bad traffic coming from Germany broke the User Environment rule. By the end of July, violations of the User Environment rule had increased by **22,050%**.

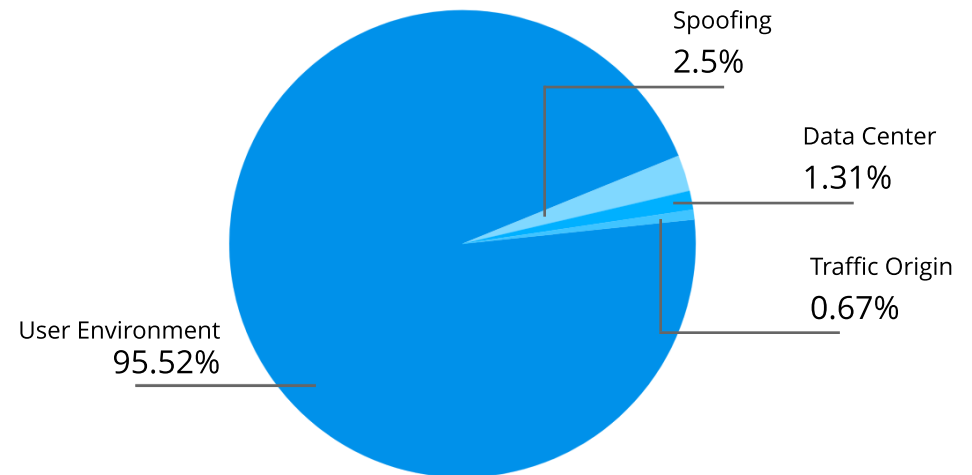
Germany's top regions with the highest amounts of traffic included:

- North Rhine-Westphalia
- Baden-Württemberg
- Bavaria
- Land Berlin
- Hesse

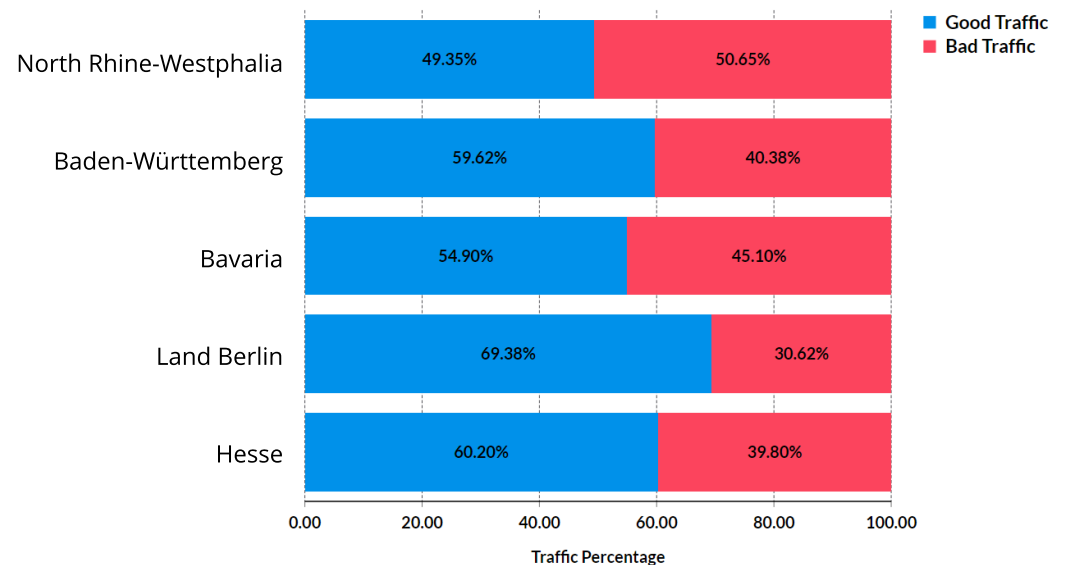
High populations coupled with rapidly growing technology and manufacturing industries can attribute to why these five regions topped the list.<sup>6</sup>

Of the five, North Rhine-Westphalia had the highest amount of bad traffic, with **50.65%** marked as suspect. Anura determined that **96.86%** of the bad traffic triggered the User Environment rule set.

Germany: Percentage of Rule Sets Broken



Germany: Top 5 Region Rankings Based on Traffic





# France

Compared to the other countries in our study, France had the lowest average percentage of fraudulent traffic from May to July.

The percentage of bad traffic detected by Anura remained steady month-over-month for this country. In May, **30.12%** of all traffic passing through Anura was flagged as bad. This number dropped to **28.07%** in June, then rose again to **30.99%** in July.

Analyzing Anura's rule sets, User Environment pinged the most at **44.8%** but fluctuated dramatically. From May to June it increased by **202%**, then from June to July dropped by **46%**.

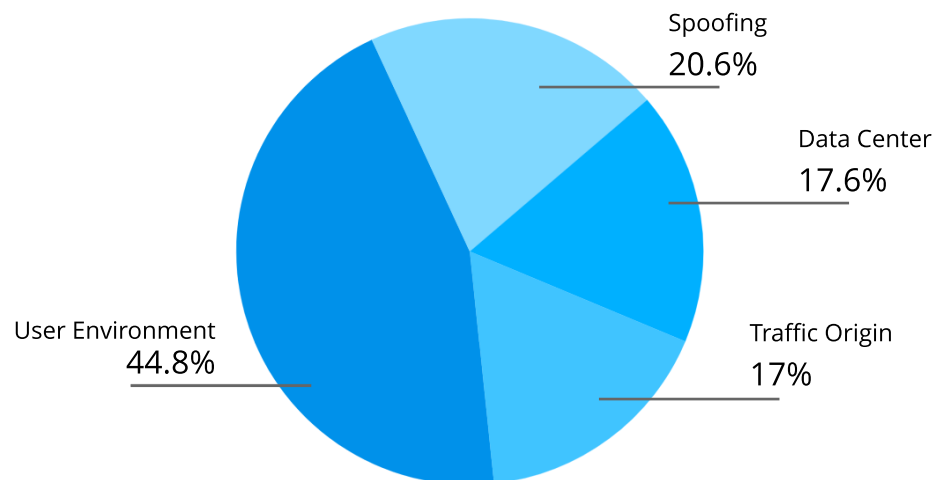
France's top regions with the highest amounts of traffic included:

- Île-de-France
- Non-identifiable
- Hauts-de-France
- Auvergne-Rhone-Alpes
- Provence-Alpes-Côte d'Azur

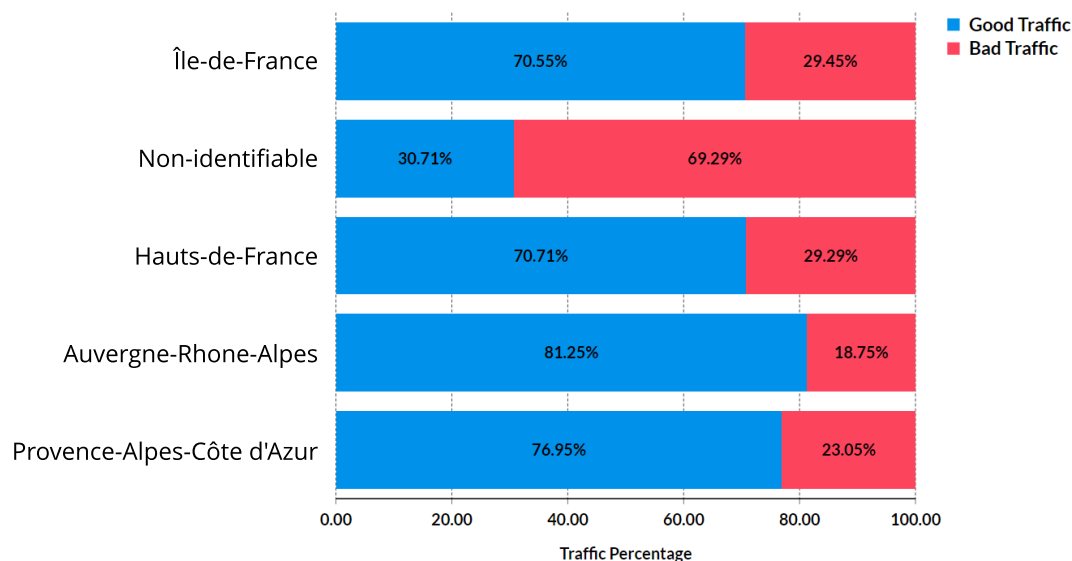
Anura recorded some regions as Non-identifiable, a label that indicates the platform doesn't have enough information to accurately mark where the traffic originated. These unknown regions triggered the highest percentage of bad traffic at **69.29%**.

The Île-de-France region, which includes Paris and its surrounding suburbs, had the second highest bad traffic percentage at **29.45%**. Around **87.2%** of that traffic broke Anura's User Environment rule set.

France: Percentage of Rule Sets Broken



France: Top 5 Region Rankings Based on Traffic



# United Kingdom

Over in the United Kingdom, from May to July, the amount of bad web traffic triggering Anura's User Environment rule set increased by **1,132%**. Given the U.K.'s ever-growing tech economy, this increase in traffic numbers isn't too surprising.<sup>7</sup>

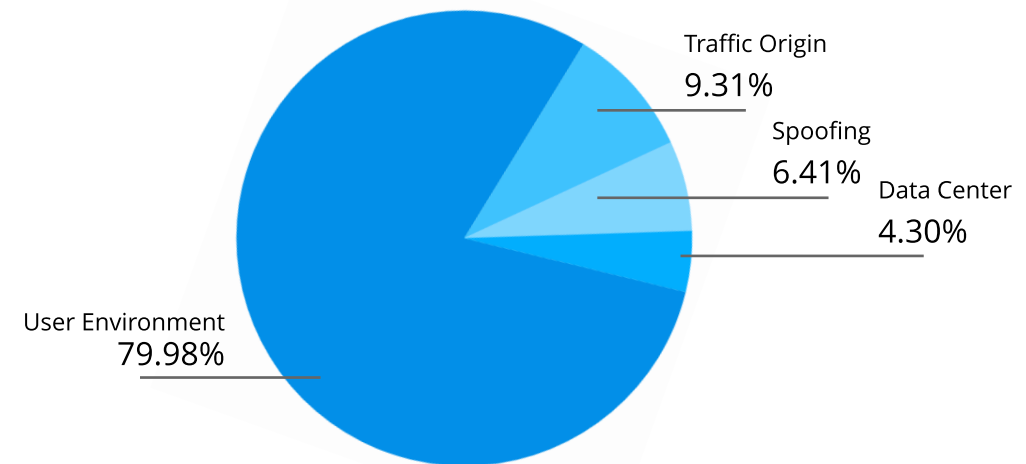
Like Germany and France, the total percentage of bad traffic didn't significantly shift over the course of the study. The percentage in May reached **35.87%**, rose to **45.71%** in June, then dropped to **21.76%** in July.

The United Kingdom's top regions with the highest amounts of traffic included:

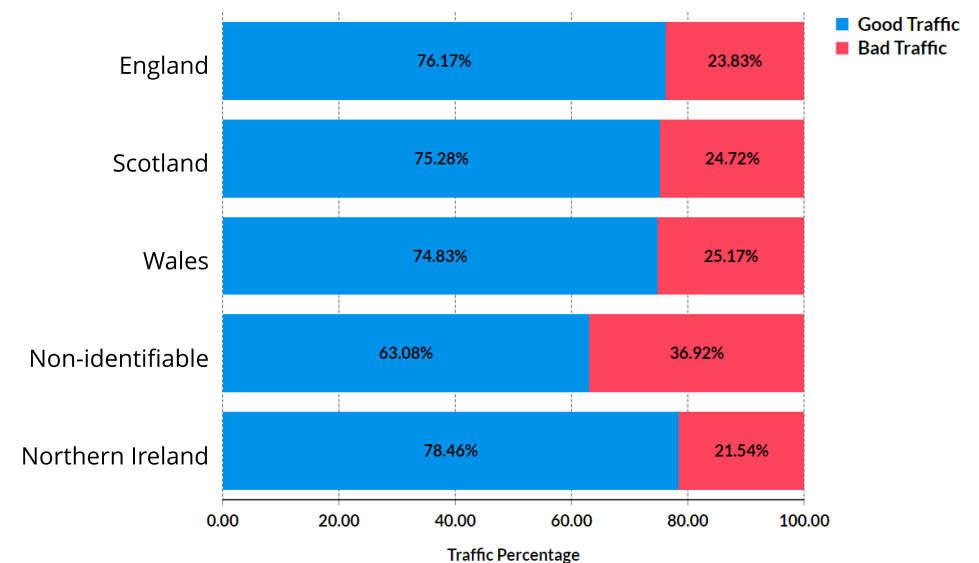
- England
- Scotland
- Wales
- Non-identifiable
- Northern Ireland

Similar to France's data set, Anura also recorded some regions as Non-identifiable due to lack of information. Again, these unknown regions collected the highest percentage of bad traffic at **36.92%**. In comparison, Wales trailed behind at just **25.17%**.

## United Kingdom: Percentage of Rule Sets Broken



## United Kingdom: Top 5 Region Rankings Based on Traffic



# How Bad Traffic Affects Marketers

Undoubtedly, fraudulent traffic has a negative effect on both branding marketers and performance-based marketers.

To gauge campaign success, branding marketers heavily rely on click-through rate (CTR), which is the number one metric targeted by fraudsters. Whenever malicious bots interact with ads, a brand's message isn't being seen by real users. Customers will only be drawn to a brand if they're actually seeing it.

Meanwhile, performance-based marketers are spending money on lead generation techniques, only to find that ad fraud is watering down their ROI, essentially leaving them spinning their wheels and burning through budgets.

Many brands choose to work with a particular ad fraud solution because that's what their clients prefer they use. Clients want an accredited solution or a solution that still lets them meet their traffic needs.

But Anura doesn't mask traffic to fit a specific direction. Our solution focuses on the user, along with performance and true branding, which separates us from other options currently available.

Most fraud solutions aren't transparent about why traffic is bad. They just give you a probability statistical scoring model, which essentially tells you it's 65-75% bad, no questions asked. They're not giving you a definitive score, just a probable score. As a result, you're left guessing, and they're not being held accountable.

But by using an ad fraud solution like Anura, you'll know exactly why the traffic was flagged, giving you the option to stop bad traffic in real-time, and more importantly, stop paying for it. Then you can take those saved ad dollars and reinvest them, making your marketing more efficient.



## Sources

<sup>1</sup> Tech and Manufacturing Driving Growth in Southern U.S. Markets, *Urban Land Magazine*, August 27, 2018.

<sup>2</sup> Tech Cities 1.0, *Cushman & Wakefield Research*, June 15, 2017.

<sup>3</sup> CBRE: 2017 was yet another record year for the European data center market, *Data Centre Dynamics*, February 21, 2018

<sup>4</sup> IAB Europe Digital Brand Advertising and Measurement Report, June 2018

<sup>5</sup> UKOM Digital Market Overview, *IAB U.K.*, May 4, 2018

<sup>6</sup> Industries in Germany, *Germany Trade and Invest*, September 2018.

<sup>7</sup> UK tech sector growing 2.6 times faster than overall economy, *Computer Weekly*, May 17, 2018.



Anura is an ad fraud protection solution that monitors your traffic to identify real users versus bots, malware, and human fraud. Built and optimized on customer conversion data since 2005, Anura excels in conversion-based campaigns, finding more fraud with greater accuracy. Our integration offers complete transparency with a full Analytics dashboard to identify bad traffic by a variety of metrics.

For more information, visit [anura.io](https://anura.io) or contact sales at 888.337.0641 or [sales@anura.io](mailto:sales@anura.io)