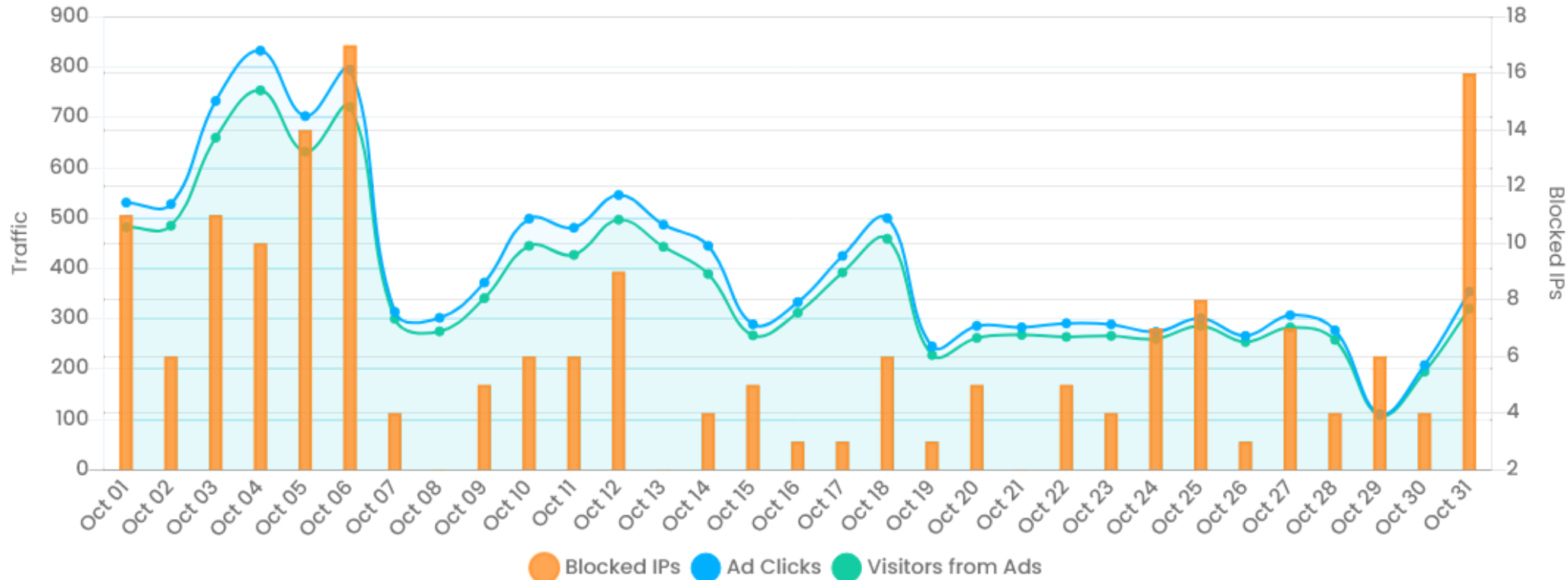


ClickCease Monthly Report for artisanserrurier.lu

October 1 – October 31



Visitor & Click Analytics



This graph shows the trend for the 3 main KPIs: visitors from ads, clicks, and blocked IPs.

On **Oct 05**, **Oct 06**, and **Oct 31** there was more than twice the amount of fraud detected than the average for the month. There was an unexpected spike in fraud during this period. ClickCease has detected the attack and blocked the IPs involved.

Analytics

Ad Clicks**12608**

Total paid ad clicks between **October 1** and **October 31**.

Detected IPs**198**

Between **October 1** and **October 31**, **198** IPs have been detected and blocked from your Google Ads campaigns.

Detection Rate**1.6%**

Represents the percentage of total ad clicks that have been blocked for being fraudulent.

Savings**€263.7**

ClickCease has blocked **€263.7** worth of fraudulent traffic during this period. This money can now be spent on genuine traffic going forward.

ClickCease improved your ad Spend by generating **1.6%** cleaner traffic for **artisanserrurier.lu**. This will result in an increase in genuine clicks that will boost the performance of your ad campaigns.

Detected IPs

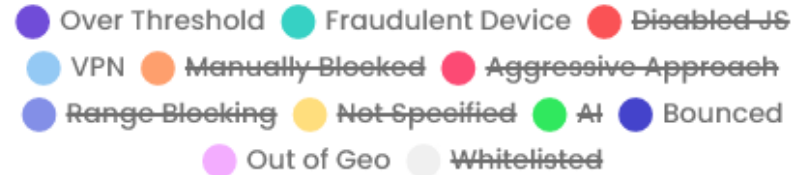
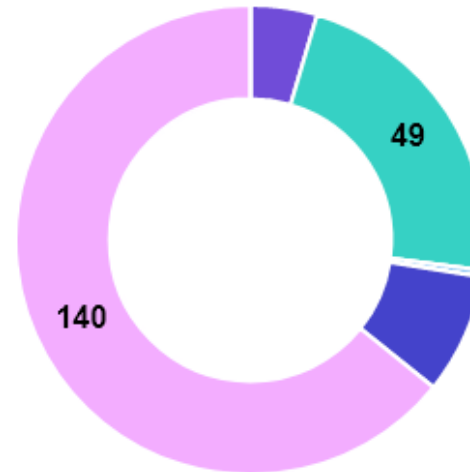
Top reasons for blocked IPs:

Out of Geo

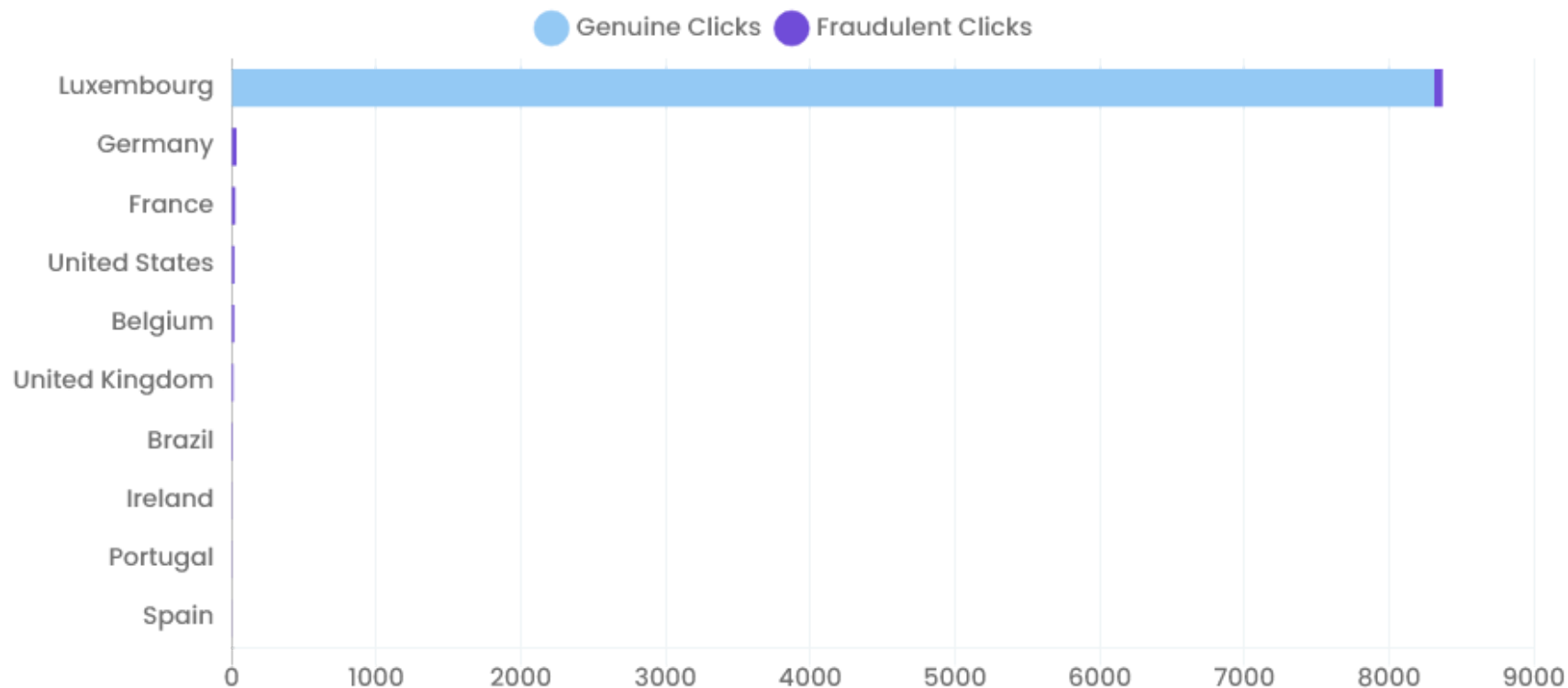
64.2 % of your fraud is coming from foreign countries that you are not advertising to. Google's geo-targeting is not perfect, if an IP is detected from a country that you do not want clicks from, we will block it right away and mitigate the damage.

Fraudulent Device

22.5 % of your fraud is comprised from repeat offenders. We assign every device a unique ID. If a competitor or bot changes their IP, we will still be able to catch the device ID and block the fraudster immediately.



Top Fraudulent Countries



Your fraud arrives from a number of different countries without a primary culprit.

We have a Block by Country feature that we can set to auto-block any clicks outside of **Luxembourg** and any other countries you are targeting.

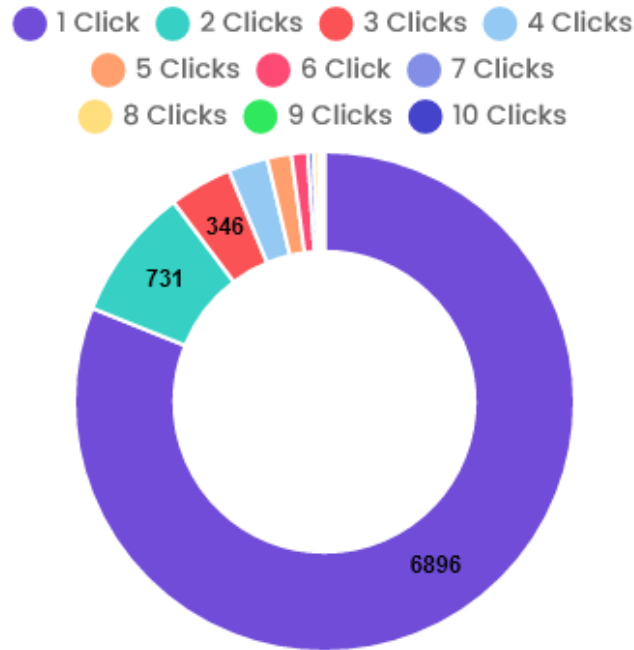
Top Fraudulent Keywords

Looks like there's no data to display



Try extending the range to see keywords

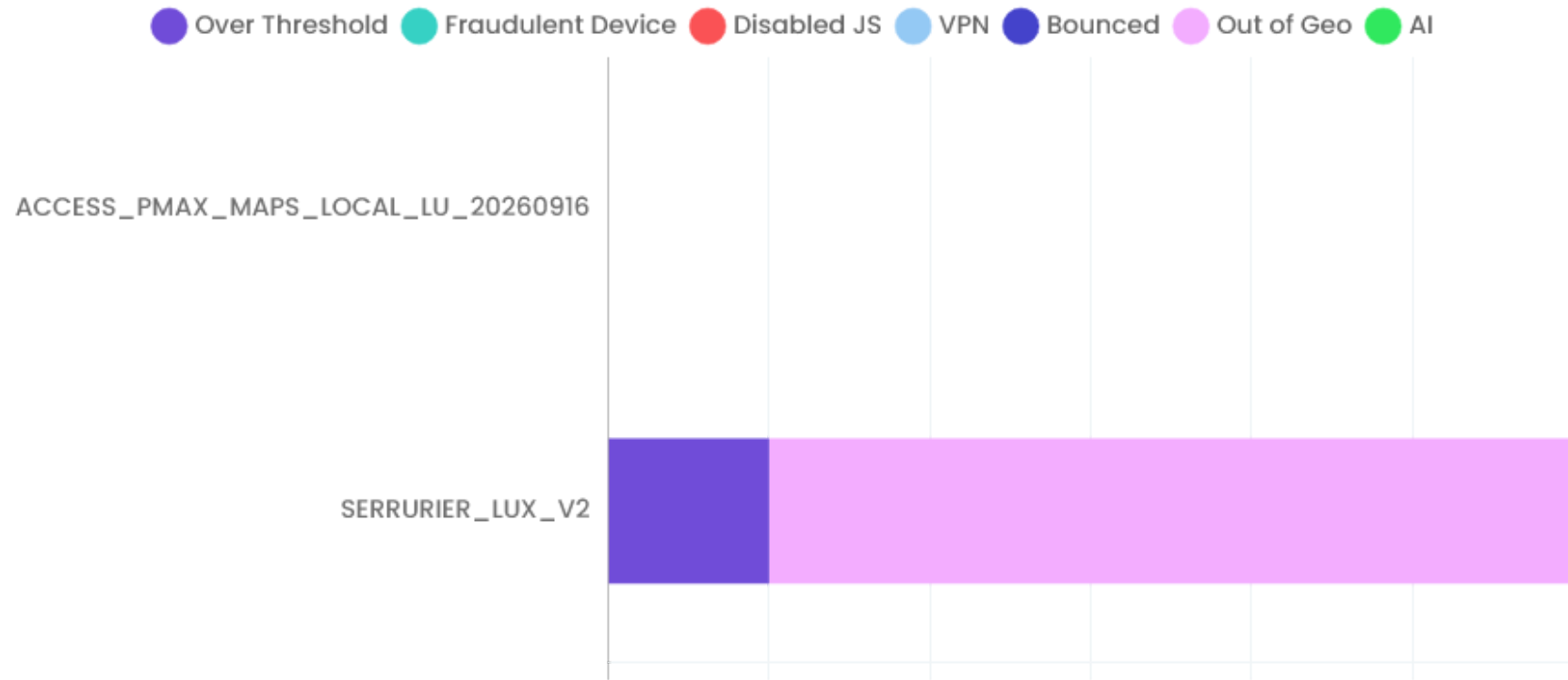
Multi-clicks



CLICK	CLICKS	PERCENTAGE
1 Click	6896	81.02%
2 Clicks	731	8.59%
3 Clicks	346	4.07%
4 Clicks	217	2.55%
5 Clicks	133	1.56%
6 Clicks	89	1.05%
7 Clicks	32	0.38%
8 Clicks	29	0.34%
9 Clicks	11	0.13%
10+ Clicks	19	0.22%

Each section represents how many times a unique IP clicked on your paid ads. This helps set a click fraud threshold that fits your traffic and business needs. **81.0%** of traffic for **artisanserrurier.lu** is only clicking 1 time. Only **0.22%** of your traffic is clicking more than **9 times** on your ads. We can safely set your threshold **from 5-10** without risking genuine traffic.

Top Fraudulent Campaigns



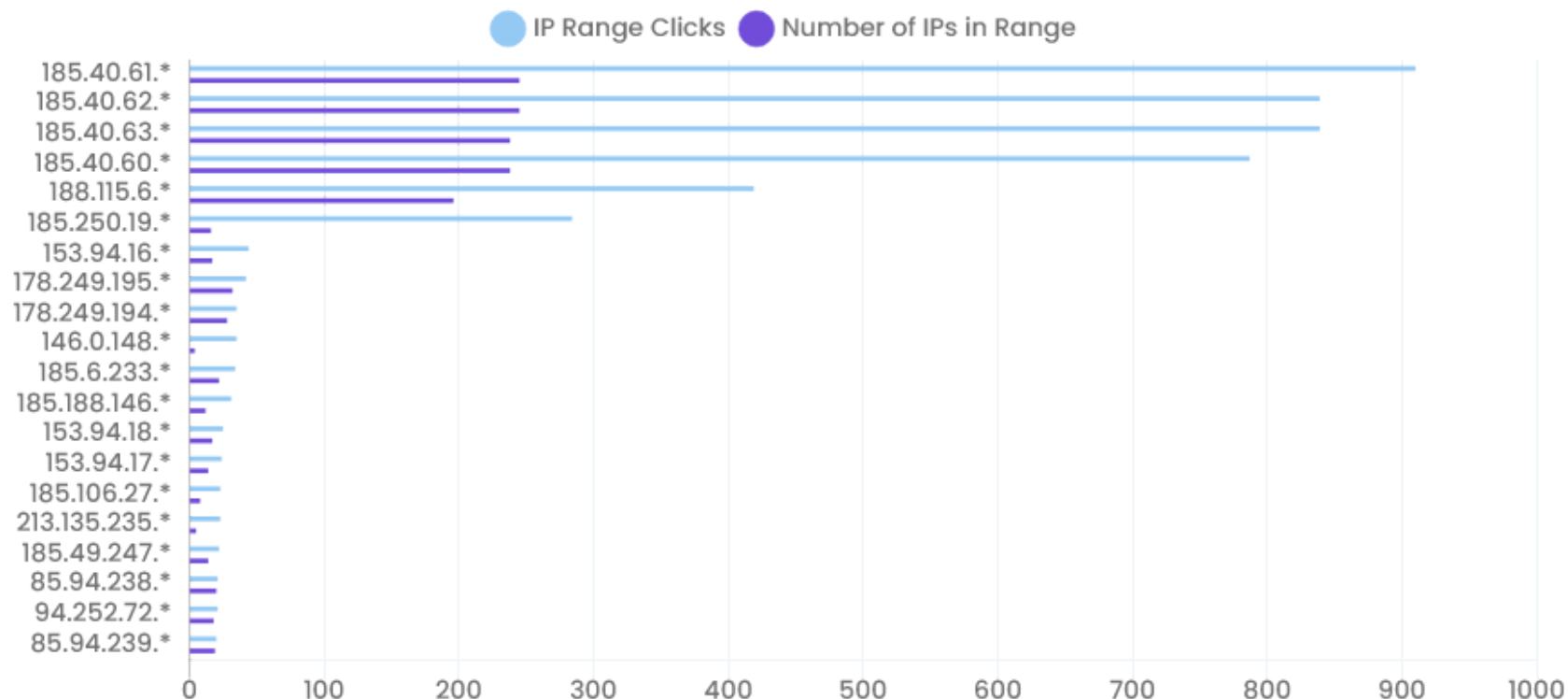
The campaigns that have been affected the most by fraud are:

ACCESS_PMAX_MAPS_LOCAL_LU_20260916 (0.0%)

SERRURIER_LUX_V2 (100.0%)

The most prevalent reasons for detection on these campaigns were **Over Threshold** and **Out of Geo**, respectively.

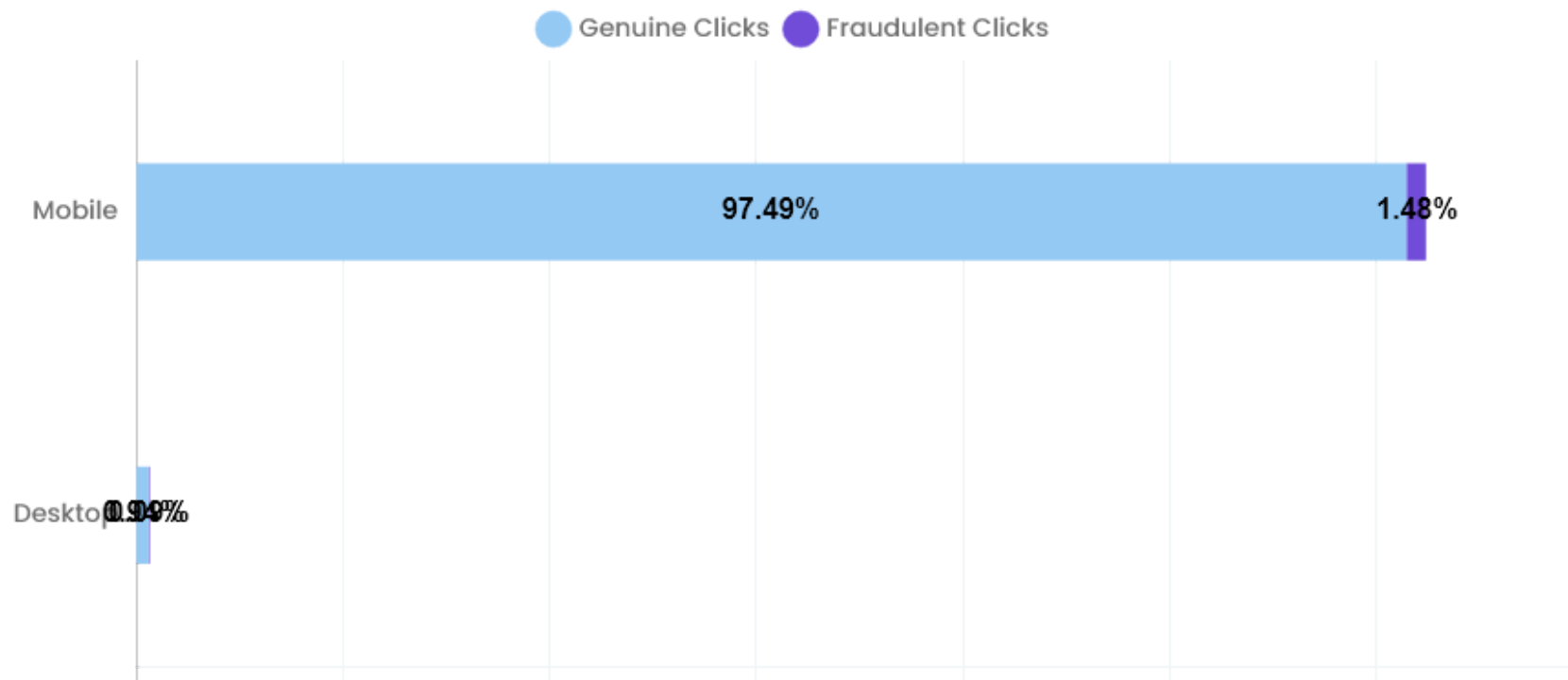
Top Clicking IP Ranges



185.40.61.* is the top clicking IP range with **910** clicks by **245** IP Addresses.

The chart above represents the amount of clicks that are coming from the top IP Ranges and how many individual IPs are coming from that range. When there is a large discrepancy between total clicks and total IPs used it is an indicator that competitors or a bot network are attacking your advertisements. IP Range Exclusion is currently disabled in your account. This feature will automatically block IP areas with high rates of fraud.

Mobile vs Desktop



There is a major discrepancy between Desktop and Mobile. Mobile accounts for a staggering **94.4%** of fraud detected on the account. It is easier for a fraudster to change their IP on a mobile phone than it is on a desktop device. We are able to flag a fraudulent device and block it immediately, preventing a fraudster from multiple clicks from the same IP.

Domain Configuration

SETTING	CURRENT	CONFIGURED CORRECTLY?
Click Fraud Threshold	Allow up to 10 clicks in 5 days	
Minimum Seconds on Site	Disabled	✗
Device Detection	Enabled	✓
Block by Country	Enabled	✓
JS Bot Detection	Enabled	✓
VPN & Proxy	Disabled	✗
Behavior Analysis	Enabled	✓
Monitoring Only Mode	Disabled	✓
IP Range Exclusion	Disabled	✗
Campaign Level Blocking	Disabled	✓
Aggressive Mode	Disabled	✓

Domain Recommendations

IP Range Exclusion

This is a powerful feature that has the ability to block thousands of IPs from areas with high rates of fraud. We recommend disabling this feature at this time, as you are not experiencing a high amount of fraudulent ranges in the last 30 days.

Time on Site

This feature will allow ClickCease to auto-block traffic that bounces from your site in a short period of time. We recommend setting a value of **3 seconds**. This will prevent that user from damaging your campaigns further.

Threshold

Based on your volume of **12608** clicks and your multi-click rate in the last 30 days, we recommend a threshold of **3 clicks in 10 minutes** and **from 5-10 clicks in 30 days**. This will prevent competitors from spamming your ads in a short period of time, and also limit them from clicking on your ads more than 5 clicks in 30 days and wasting your ad budget.