FORENSIQ

Overview

We identified a total of **25.25** of all traffic as fraudulent. Scores in the high-risk or suspect ranges have been linked to lower quality traffic and can often be traced to fraudulent sources, sub sources, or domains.

Below is the breakdown by within each risk range.

Name	Age	Sex	Location
Dave Gamache	26	Male	San Francisco
Dwayne Johnson	42	Male	Hayward

Risk by Source

Below is a summary of fraud risk by Source sorted descending by total risk. We see several sources with elevated total risk ratio, which represents the percentage of impressions which falls into our total risk range out of the total. The total risk ratio ranges from **0.0%** to **99.98%**, which falls into our **Premium** and **Premium** aggregate risk levels respectively. More information on Risk Levels can be found in the next section.

Name	Age	Sex	Location
Dave Gamache	26	Male	San Francisco
Dwayne Johnson	42	Male	Hayward

Impressions which score in the high-risk range are associated with non-human traffic through

inconsistencies seen in the visitors behavior and device characteristics. For increased insight into scoring methodologies Forensiq provides five Reason Codes, defined below:

Reason Code	Definition
Spoofed	The user's device and browser were manipulated to resemble a different device or browser. This technique is commonly used to produce a real-life distribution of traffic and simulate traffic from multiple visitors.
IP Reputation	The IP address was historically associated with high-risk characteristics like spoofing and other patterns that correspond to proxy and botnet activity.
Hosting Provider	An IP belongs to a hosting provider's range. Unlike regular Internet Service Providers (e.g. T-Mobile, Verizon), when a visit is generated from a hosting provider's IP, it is most often associated with automated, non-human traffic.
Proxy	The IP address is a known proxy.
Automated Traffic	Identifies malicious botnet activity flagged on the user level through real-time traffic pattern analysis.

Campaign optimization can be done at the Source, Sub Source, and Domain levels. The below table provides groups the Total Risk Ratio into seven distinct Risk Levels and can be used to build blacklists.

Risk Ratio	Risk Level	Description
< 2%	Premium	High quality impression traffic. Fraudulent activity may be due to false positives, which is less than 1% in organic traffic sources.
2% - 5%	Low	Fraudulent activity is not likely. Some fraudulent activity may occur at the impression level.
6% - 10%	Moderate	Some fraudulent activity is likely, concentrated at the impres- sion level. Traffic mixing between human and non-human traffic sources is likely.
		Fraudulent activity is likely, some concentrated at the

Risk Ratio	Risk Level	Description
11% - 15%	Elevated	impres- sion level. Traffic mixing between human and non-human traffic sources is highly likely.
16% - 20%	Elevated-High	Fraudulent activity is likely to affect the entire source. Traffic mixing between human and non-human traffic sources is highly likely.
20% - 26%	High	Fraudulent activity is likely to affect the entire source. Traffic mixing between human and non-human traffic sources is highly likely.
26% - 100%	Critical	It is not recommended to buy from sources with fraud levels within this threshold.

This guide should be considered in combination with the following to create custom blacklists for each Campaign:

○ **Risk Tolerance for Fraud:** How much fraud the client is potentially willing to accept have no tolerance while others may have less stringent requirements.

○ **Price Points:** The CPMs the client wants to remain within.

○ **Volume:** The volume of traffic that the client wishes to buy.

Risk by source and domain

Grouping the data by **domain** we are able to identify several sources responsible for this fraud - below are the Top 25 source and domain groupings sorted descending by Total Risk.

Name	Age	Sex	Location
Dave Gamache	26	Male	San Francisco
Dwayne Johnson	42	Male	Hayward