

Ad **Fraud** Report by FraudScore

2024

vs. 2023 and 2022

• Patterns • Results • Consequences •

Introduction

2024 was a significant year for the digital advertising landscape. Fraudsters quickly adapted to new security measures and created new ways to manipulate attribution models, especially regarding mobile advertising. Economic fluctuations and changing advertising budgets also affected the trend of fraud by region.

In this Report, FraudScore shares:

- Percentage of global ad fraud rates and their changes versus 2023 and 2022
- Identifying most fraudulent areas and fraud methods
- Fraudulent traffic by mobile and web environments
- Details of the most impacted app categories on iOS and Android
- Key trends shaping the future of digital ad fraud

About FraudScore:

FraudScore is an independent antifraud solution. FraudScore works with brands across the globe and has provided fraud detection and prevention for all kinds of advertising campaigns (CPI, CPM, CPC, CPA, and programmatic) since 2015. FraudScore works with both mobile and web traffic, and is known for its unique approach to fraud diagnosis and elimination.

FraudScore is a SaaS provider and is not affiliated with any platforms, ad agencies, affiliate networks, advertisers, etc. FraudScore gives impartial traffic checkups and is autonomous in its evaluations.

2024 in facts

Global advertising market values are estimated to be around

US\$1.1tn
in 2024

Estimated global loss from ad fraud exceeded

\$140 billion
in 2024

[projected to rise]

Overall Fraud Rate:

40.76%

of all traffic was fraudulent in 2024



34.7%
of iOS traffic was fraudulent

41.09%
of mobile traffic was fraudulent

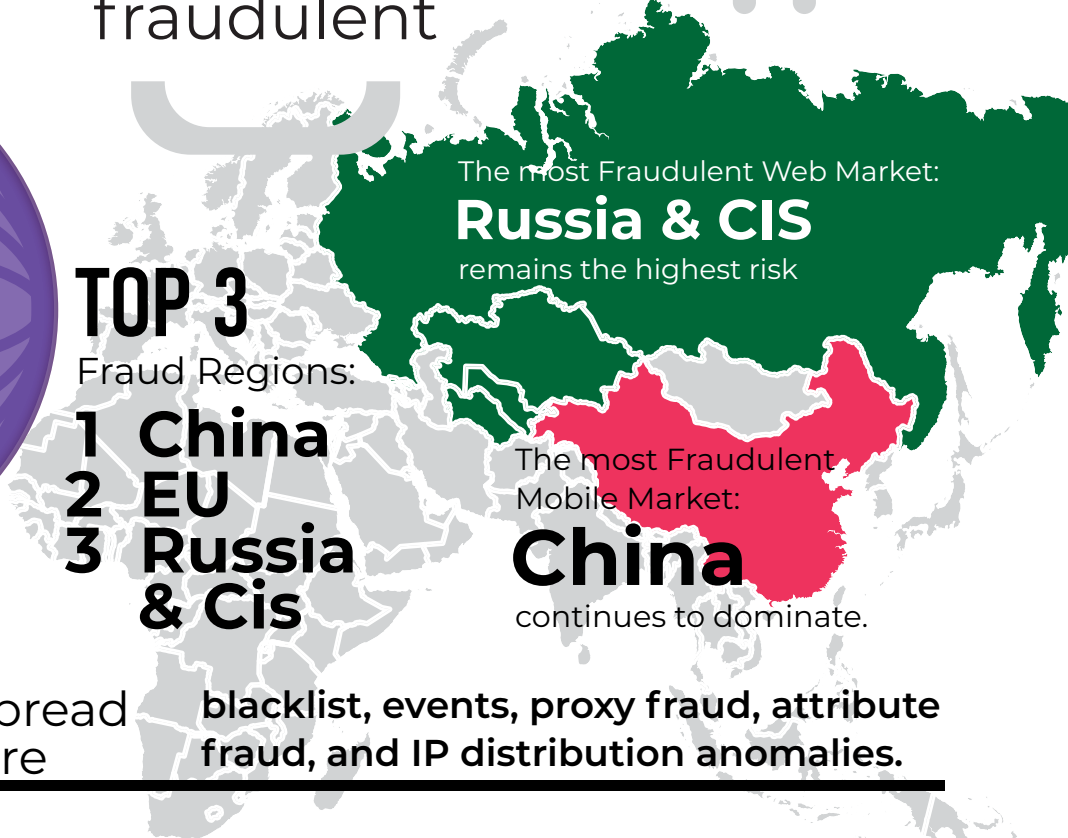


42.7%
of Android traffic was fraudulent

Web Fraud Rate:

11.03%

of web traffic was fraudulent



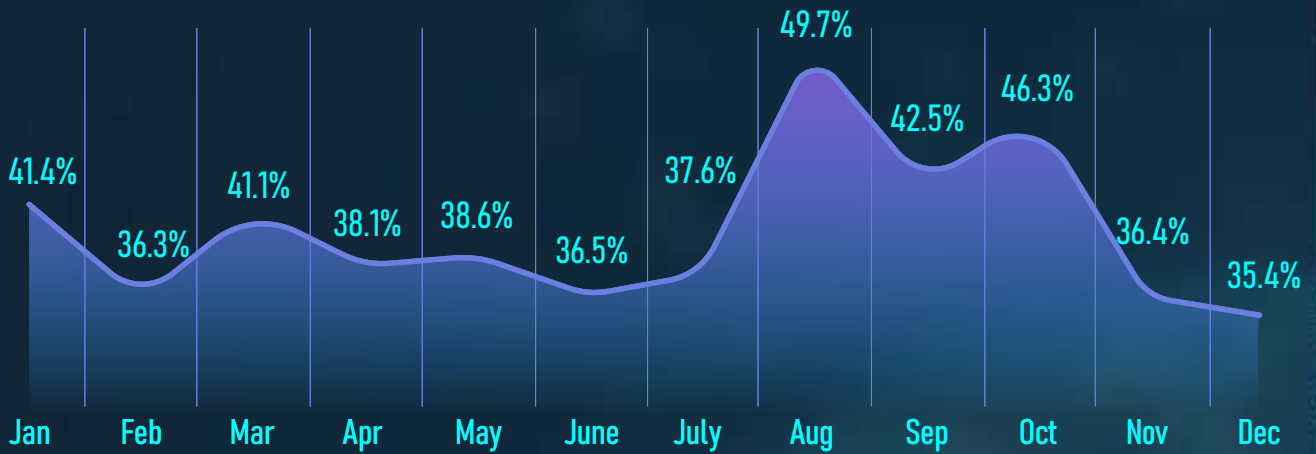
The most widespread ad fraud types are

blacklist, events, proxy fraud, attribute fraud, and IP distribution anomalies.

Ad Fraud in 2024

2024 total 40.76%

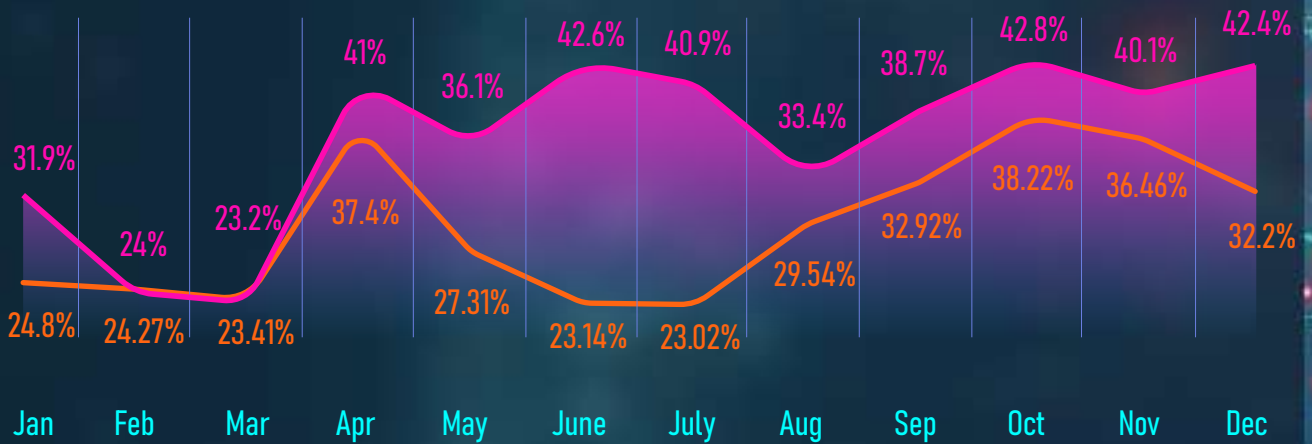
All processed traffic



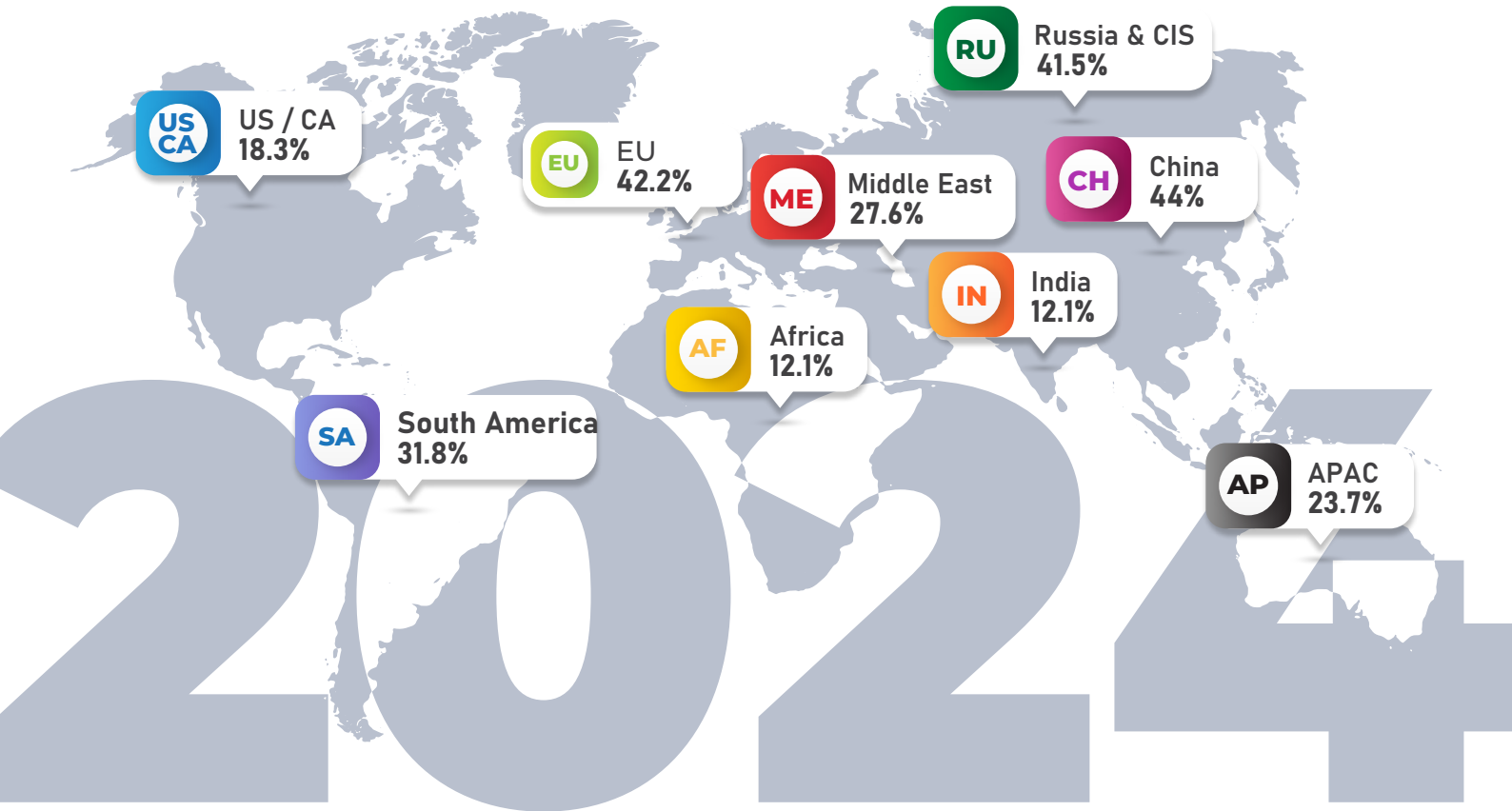
2023 total 37.71%

2022 total 29.39%

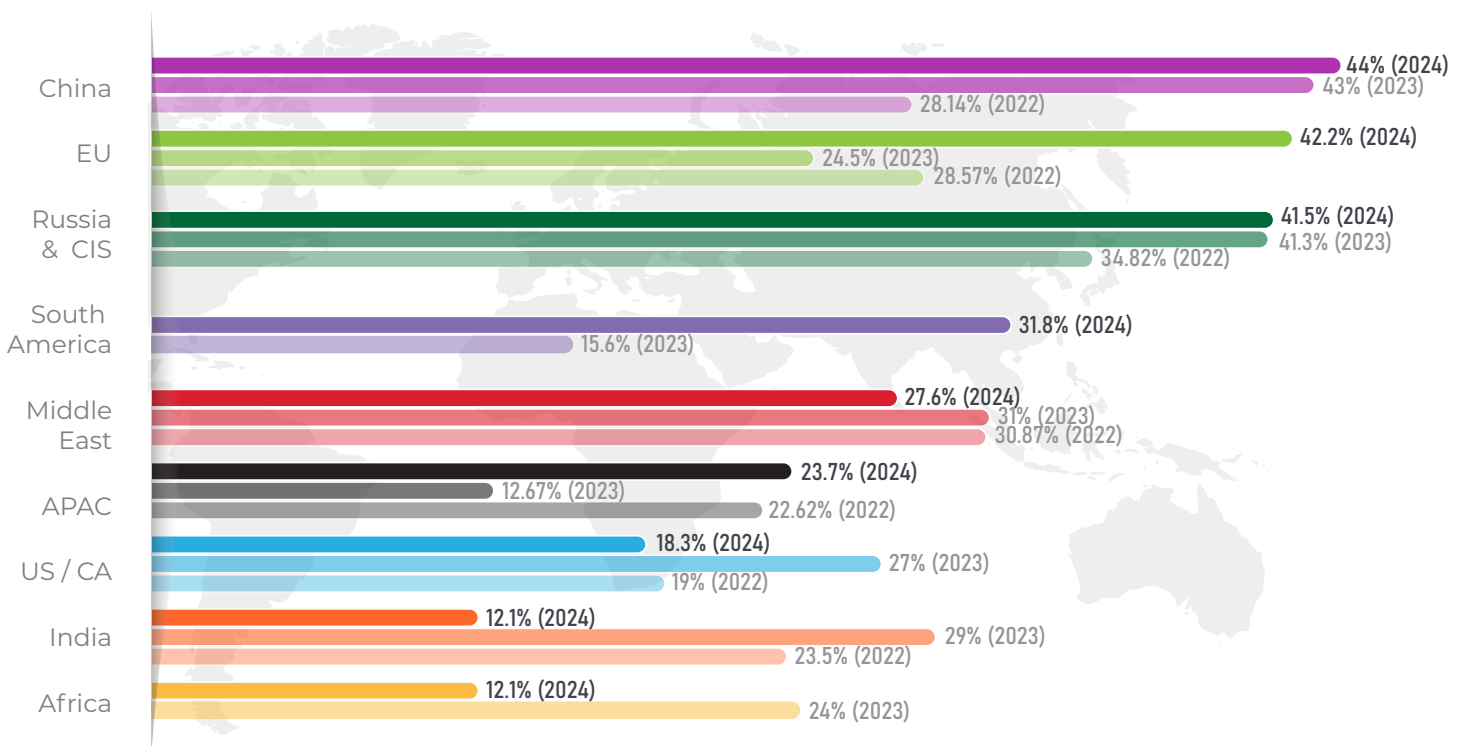
All processed traffic



2024 Geo-distribution

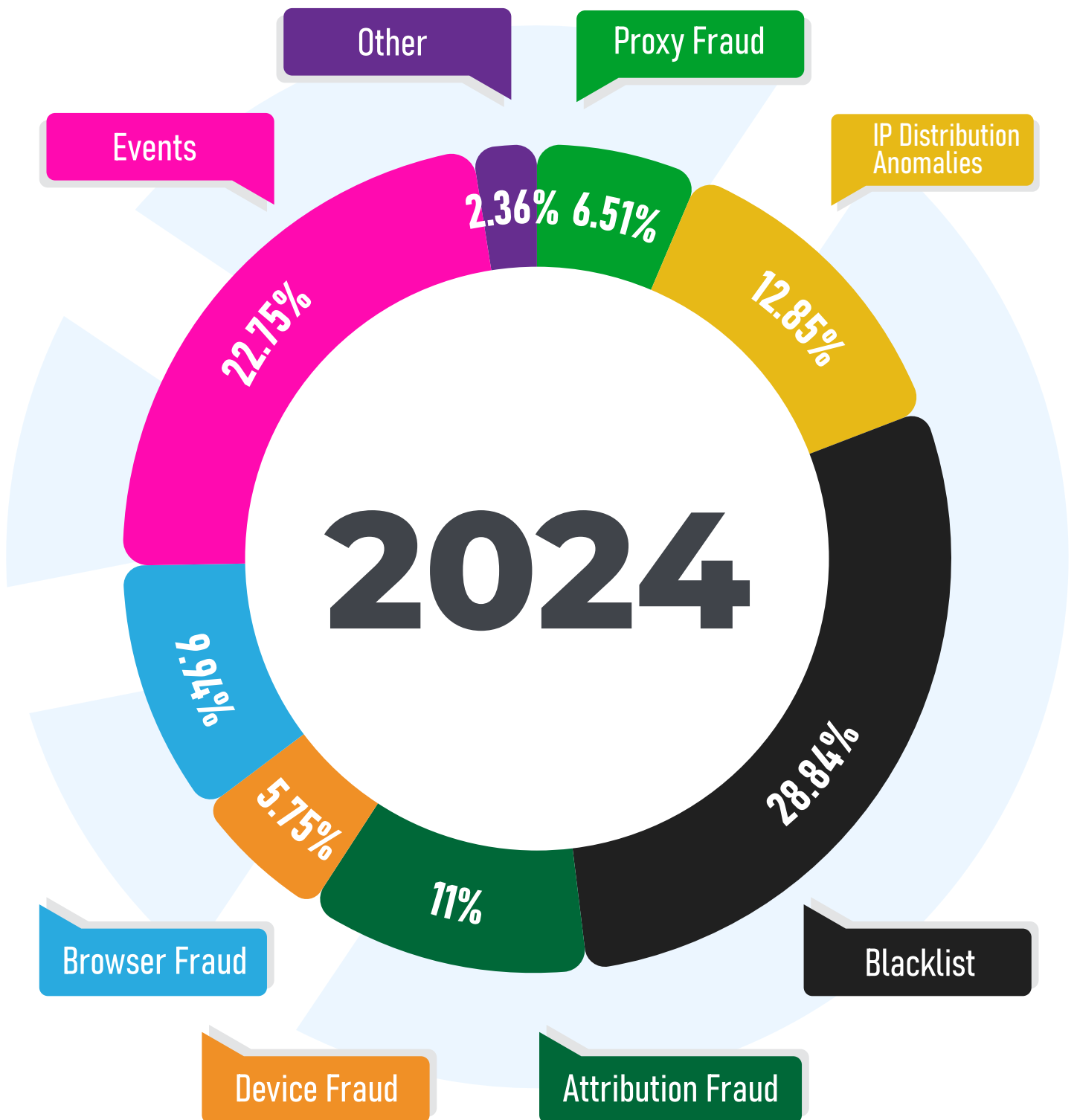


2024 / 2023 / 2022



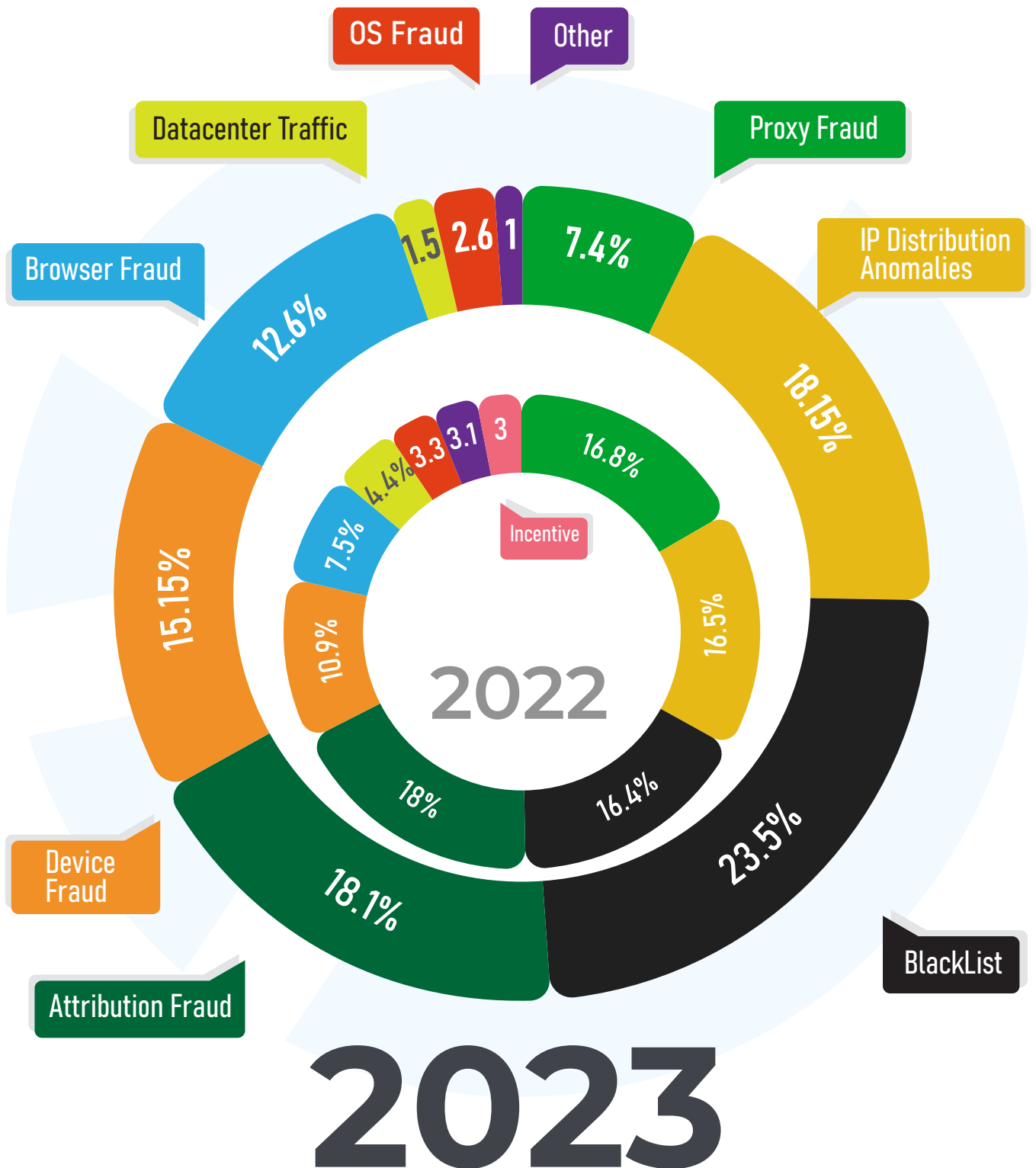
Main Fraud Categories

Distribution Ad Fraud by the Main Detected Fraud Categories



2024 Main Fraud Categories vs 2023/2022

Distribution by the Main Detected Fraud Categories

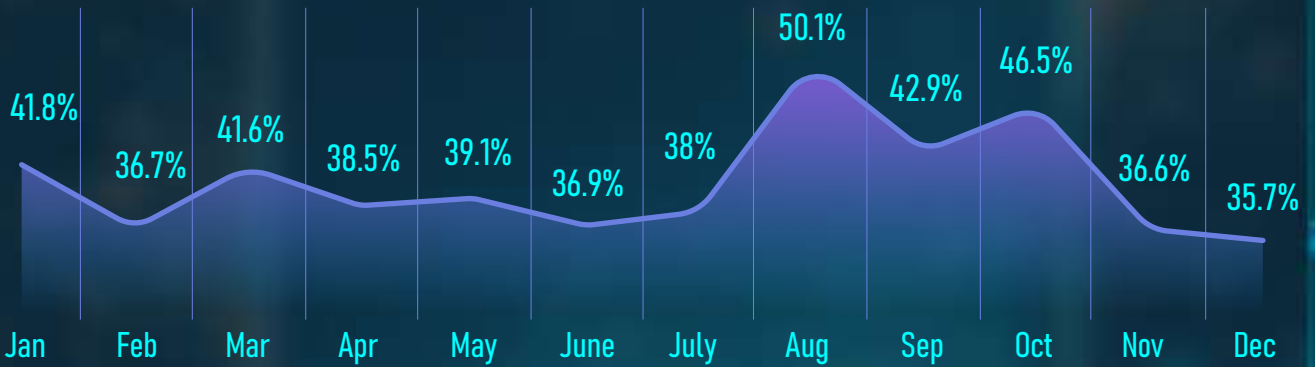


Mobile Ad Fraud in 2024

2024 total 41.09%

Mobile

% of ad fraud in global mobile traffic

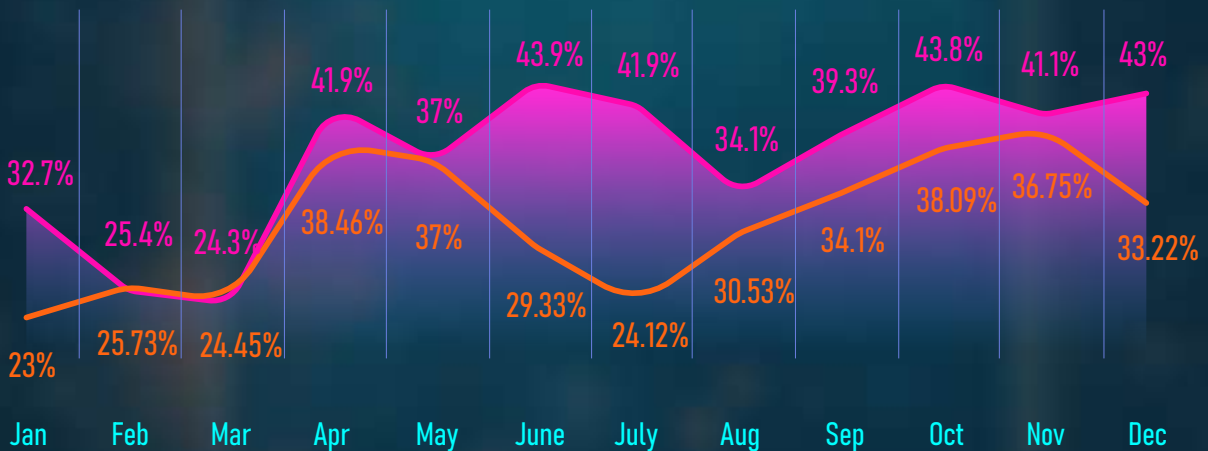


2023 total 38.65%

Mobile

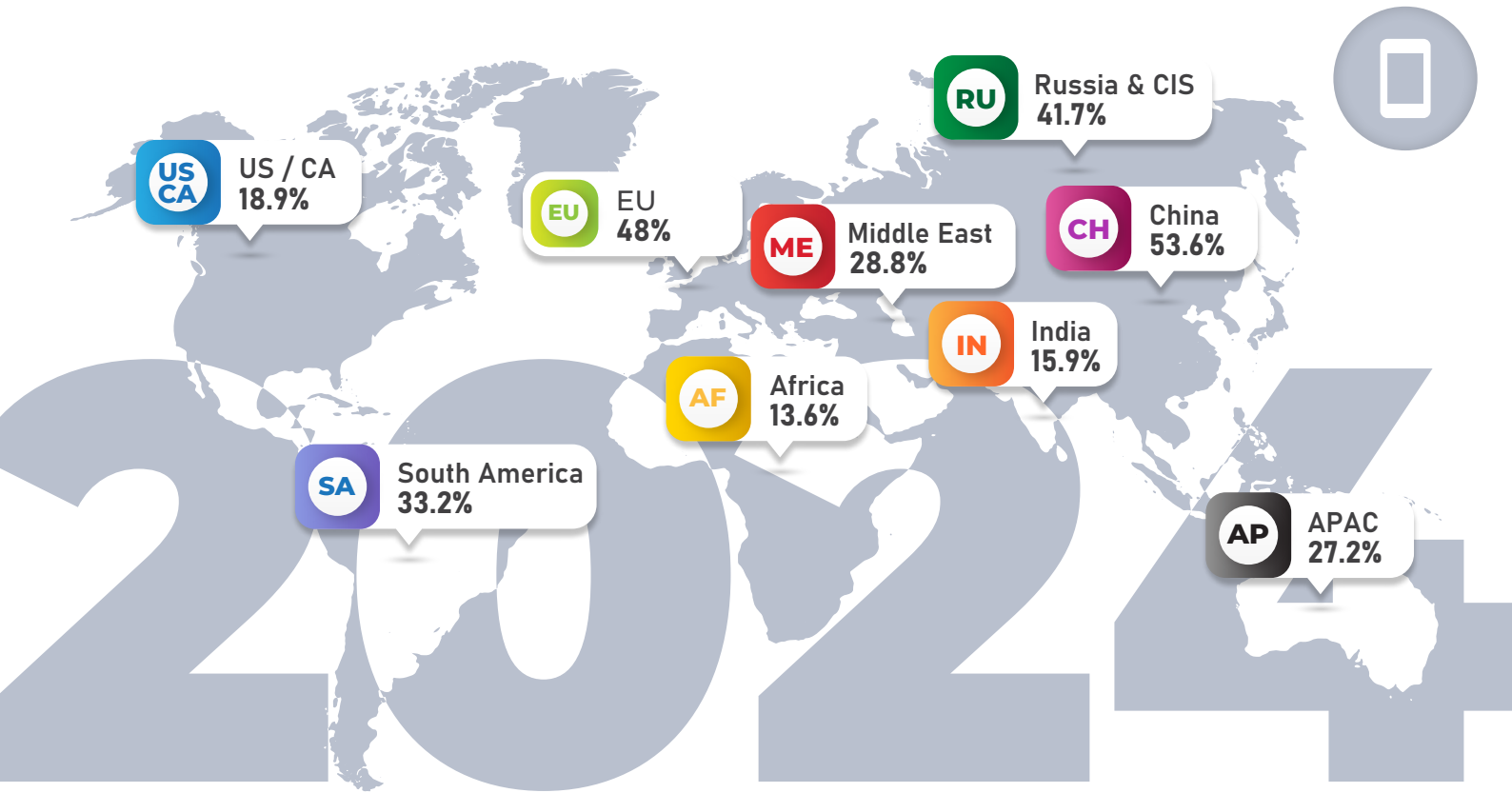
% of ad fraud in global mobile traffic

2022 total 32%

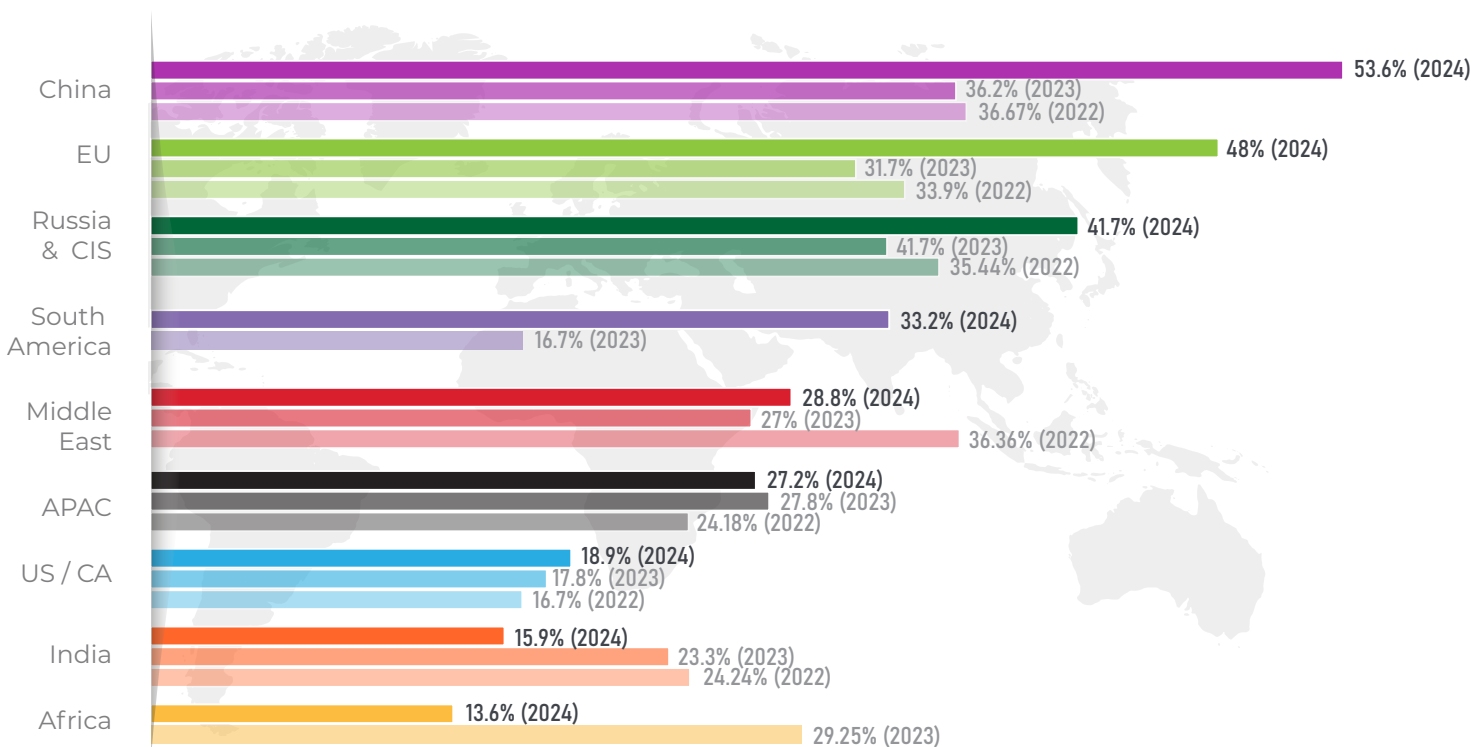


Mobile Ad Fraud in 2024

Geo-distribution

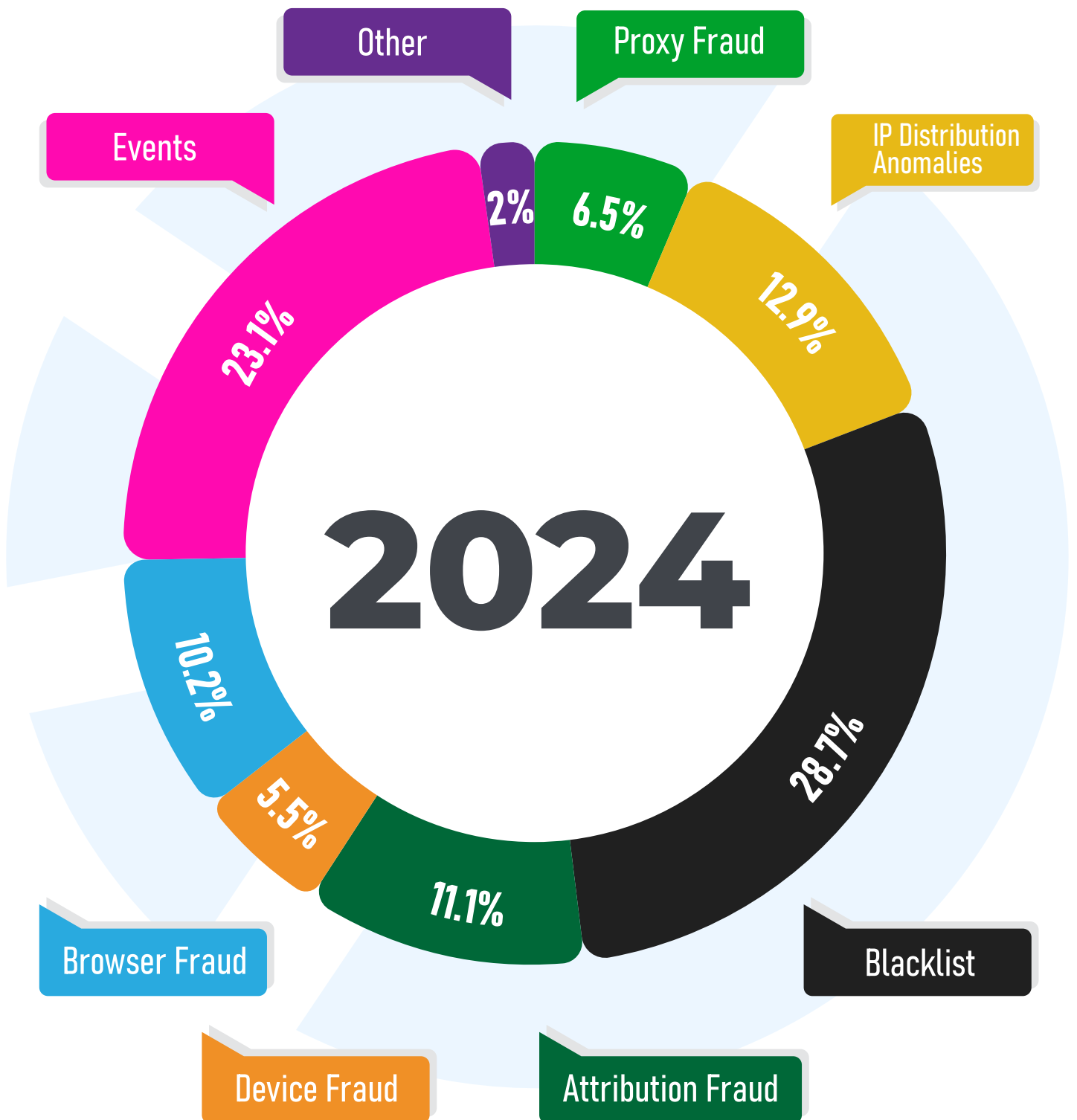


2024 / 2023 / 2022



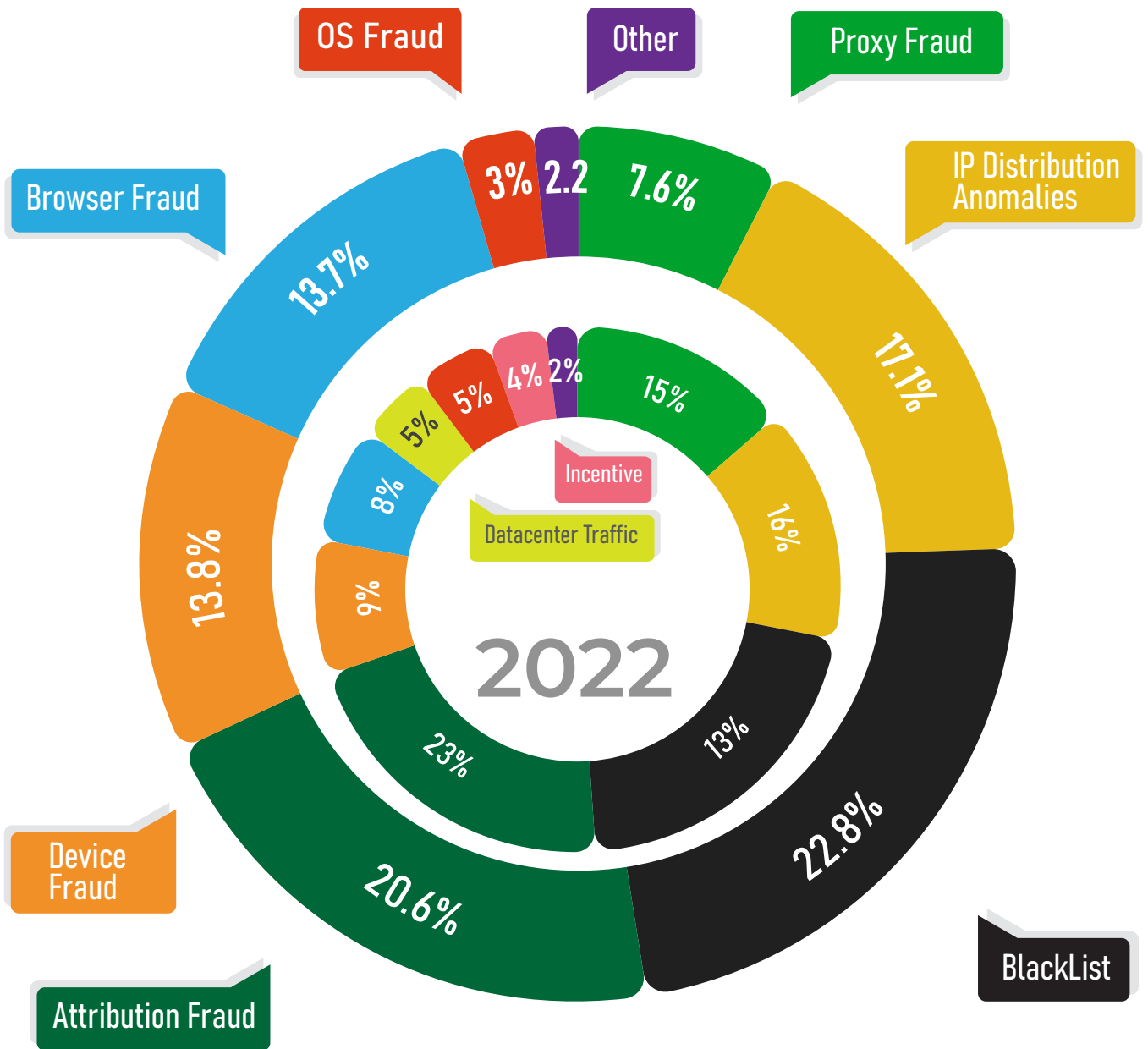
Mobile Ad Fraud in 2024

Distribution by the Main Detected Fraud Categories



Mobile Ad Fraud in 2024 vs 2023/2022

Distribution by the Main Detected Fraud Categories

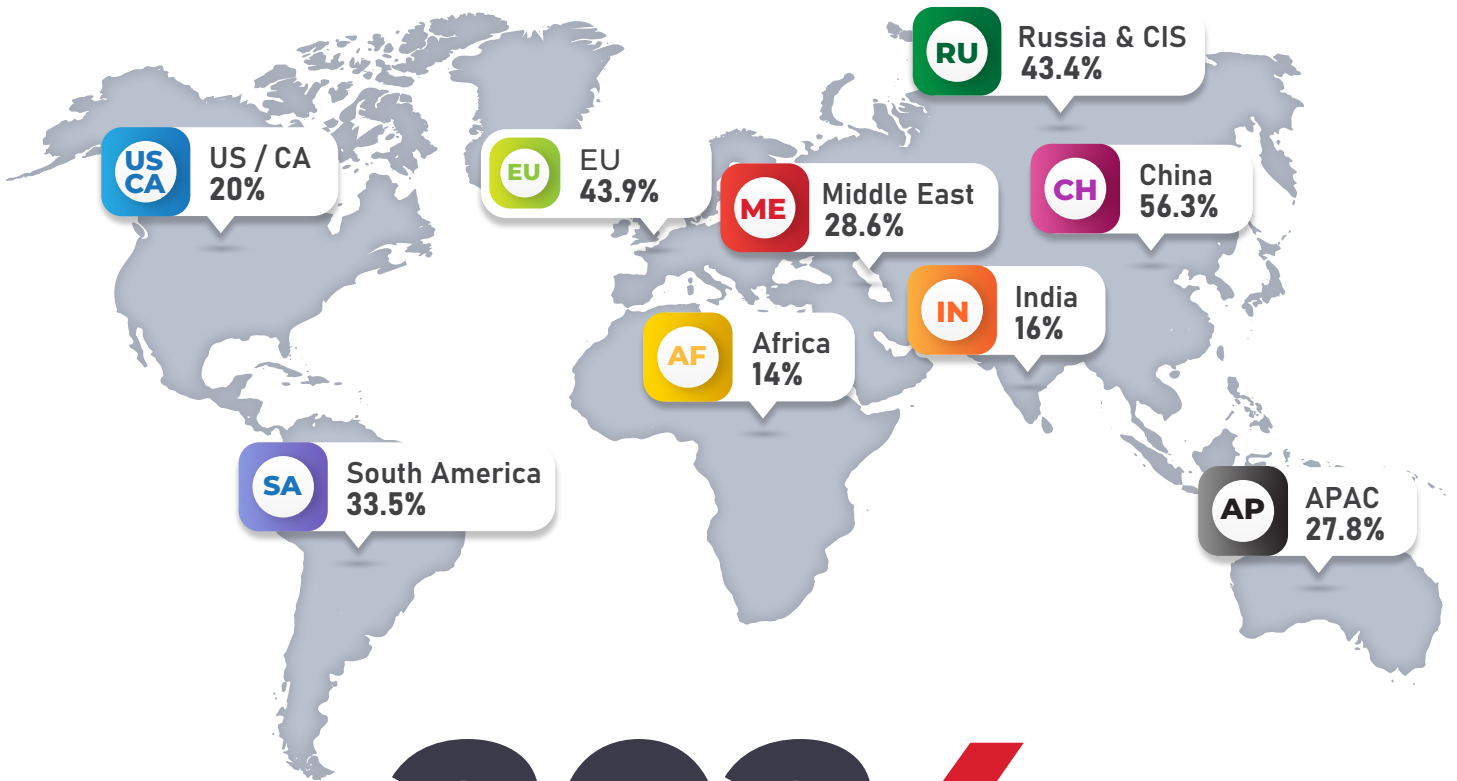


2023

Android in 2024

Geo-distribution

Total amount of ad fraud in Android traffic: **42.7%**



2024

The Most Fraud-prone App Categories on Android



47.2%

Role Playing



55.9%

Finance



35.7%

Shopping



31.8%

Maps & Navigation



31.2%

House & Home

Android in 2024 / 2023 / 2022

Geo-distribution: comparison



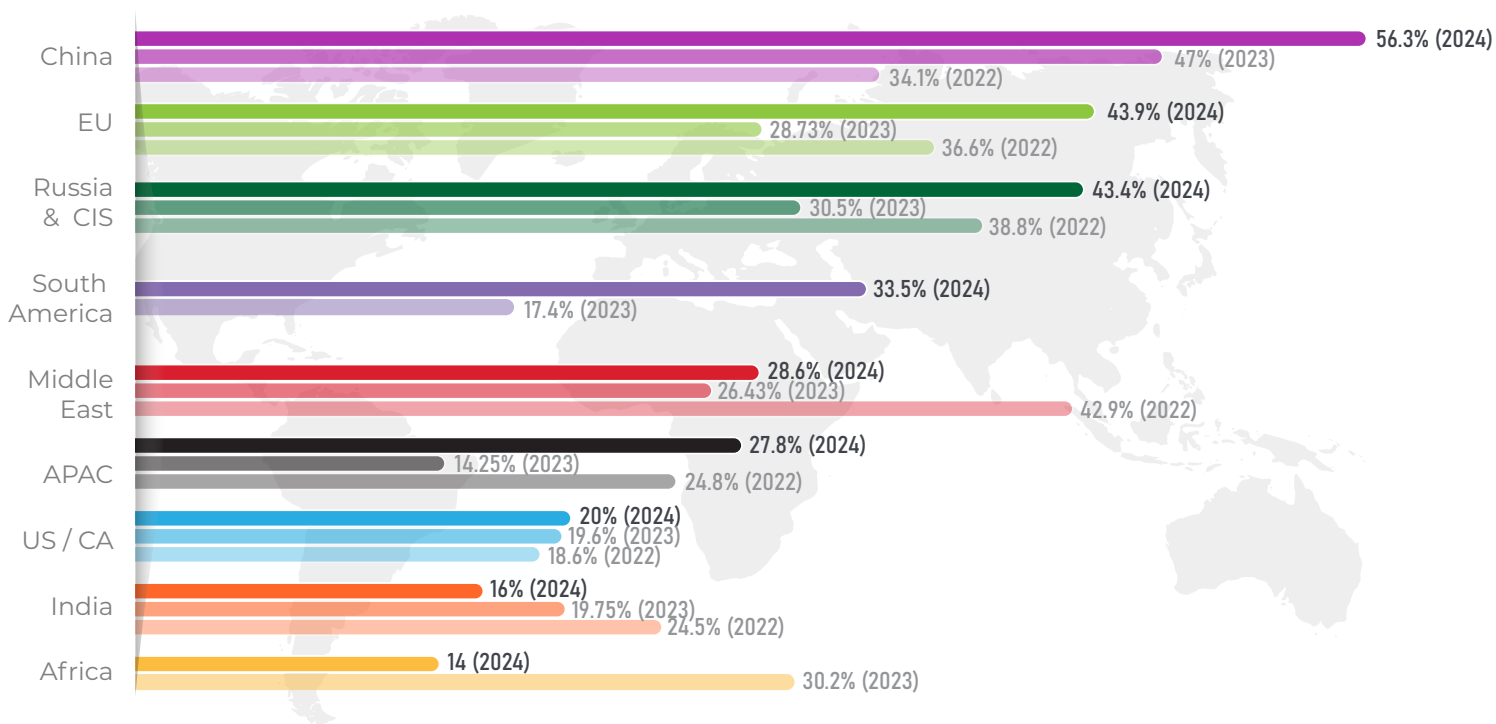
Total amount

47.2%

40.39%

31.35%

2024 / 2023 / 2022

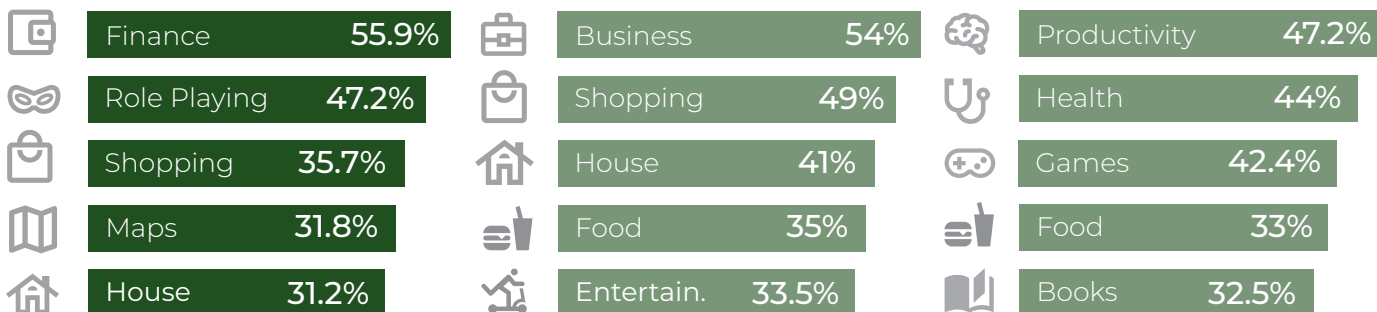


The Most Fraud-prone App Categories on Android: comparison

2024

2023

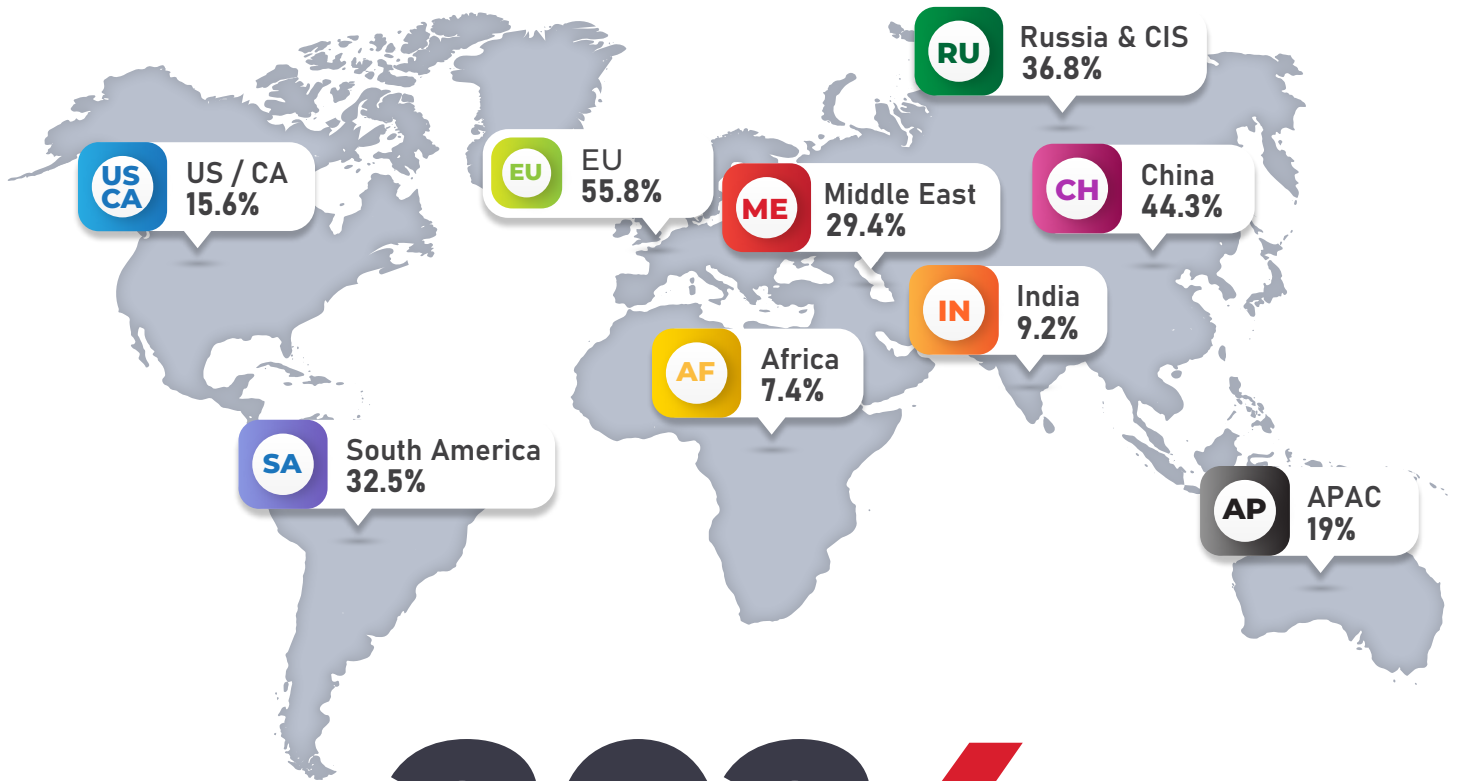
2022



iOS in 2024

Geo-Distribution

Total amount of ad fraud in iOS traffic: **34.7%**




2024

The Most Fraud-prone App Categories on Android


26.6%
Food & Drink


61.6%
Finance


25.5%
Maps & Navigation


24.8%
Travel


21.9%
Shopping

iOS in 2024 / 2023 / 2022

Geo-distribution: comparison



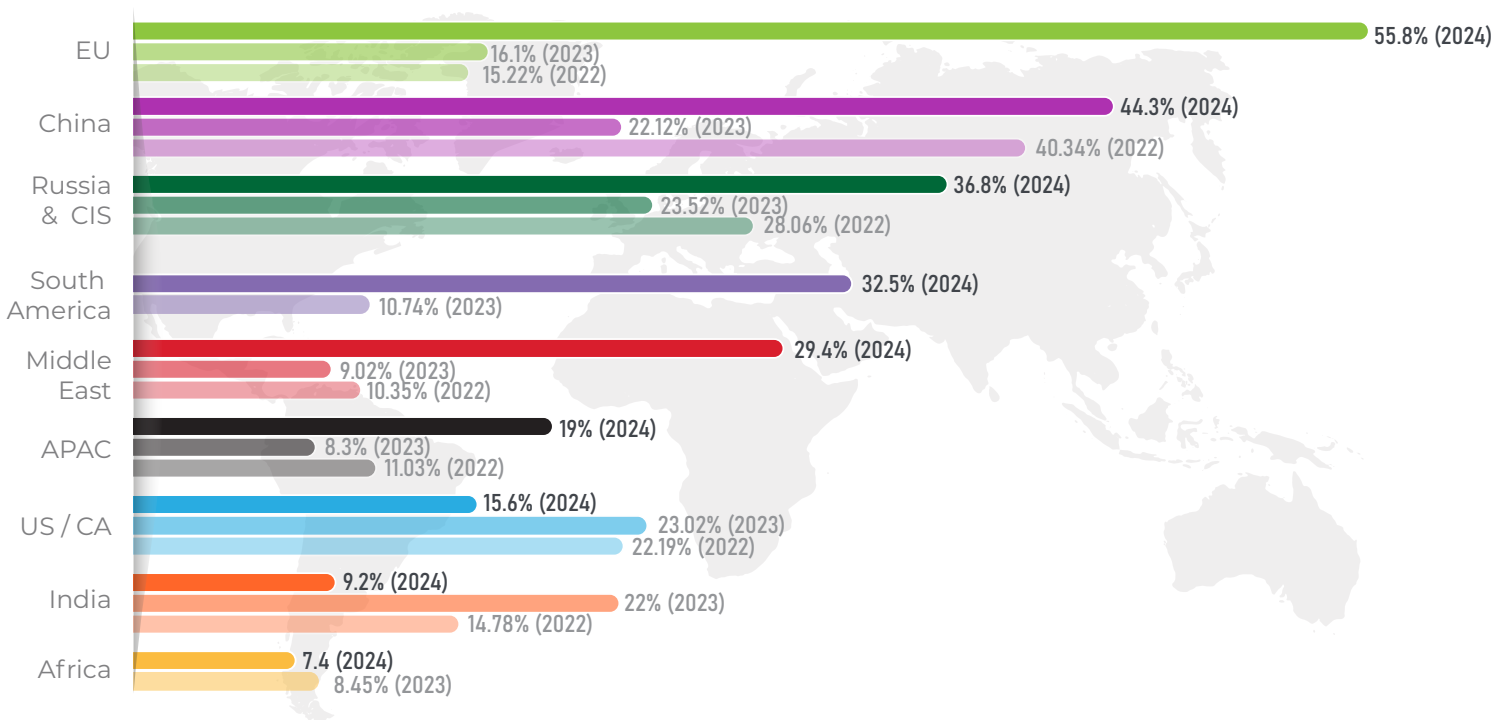
Total amount

34.7%

26.54%

29.5%

2024 / 2023 / 2022

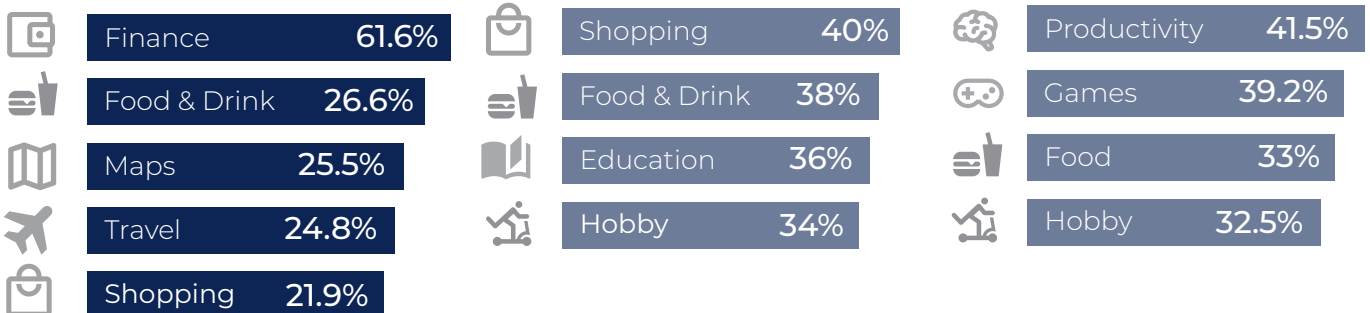


The Most Fraud-prone App Categories on Android: comparison

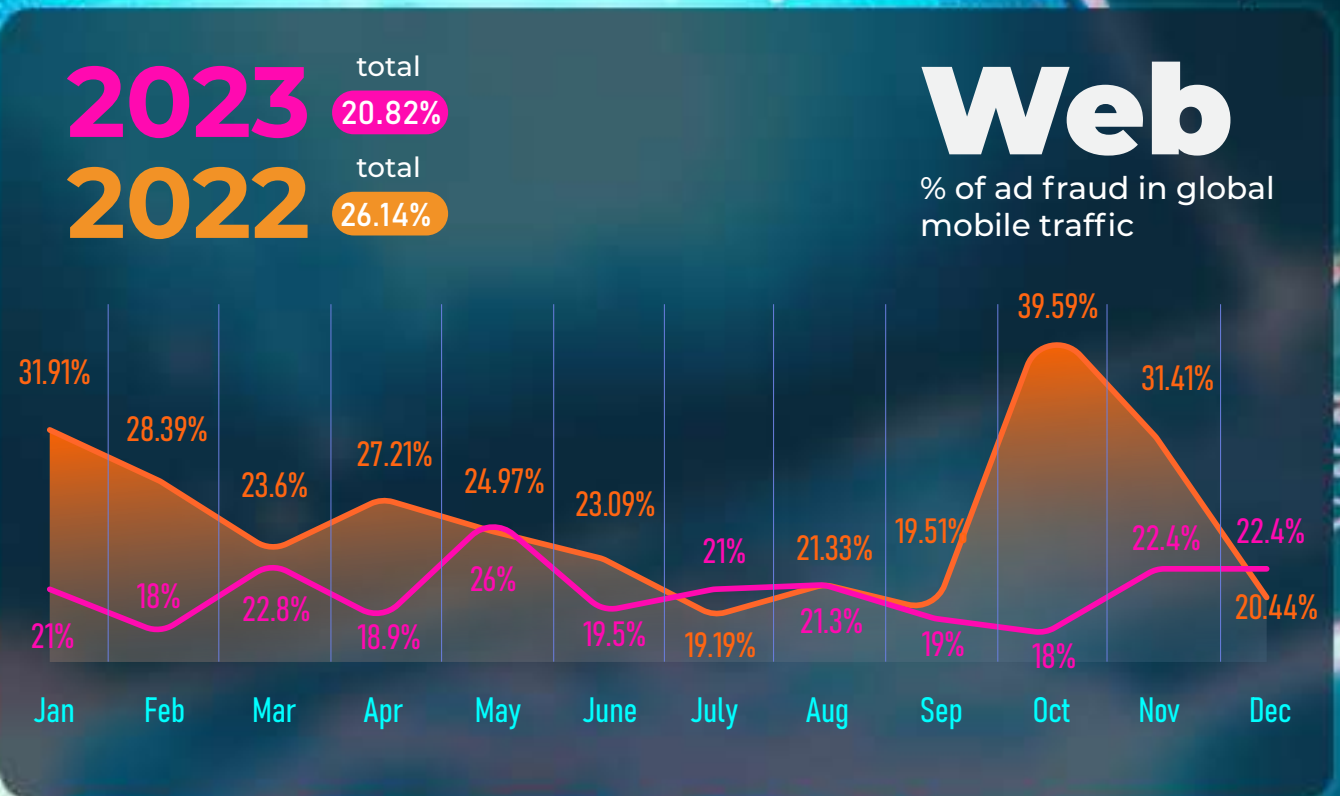
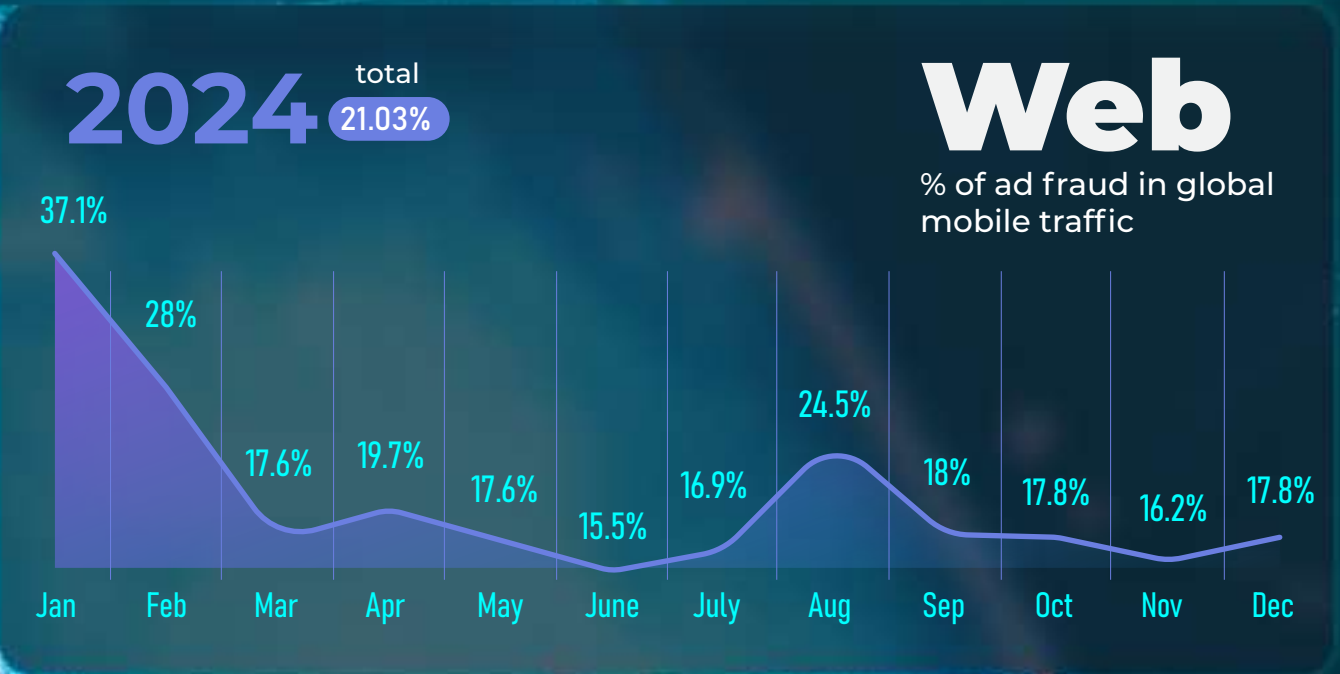
2024

2023

2022

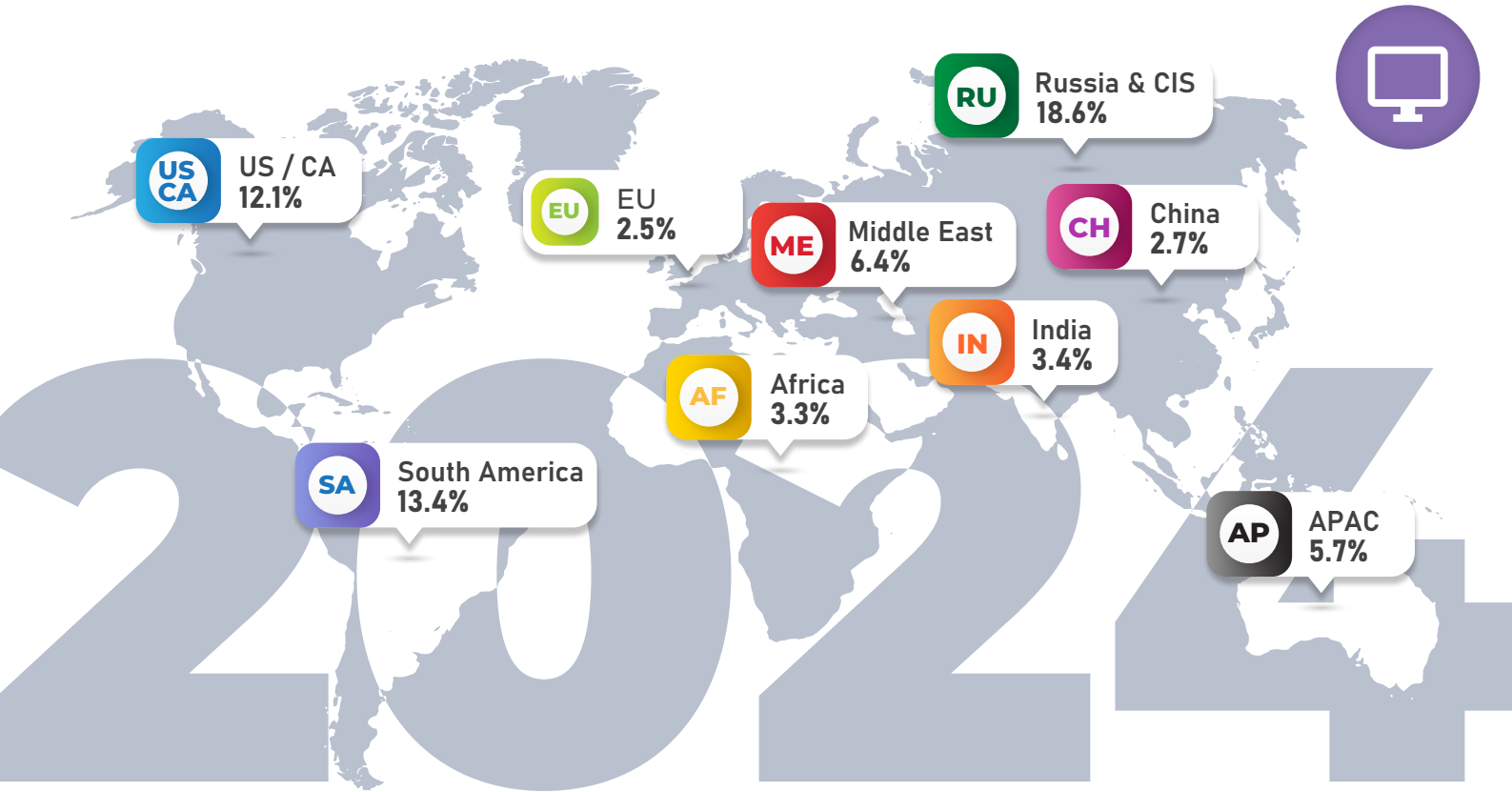


Web Ad Fraud in 2024

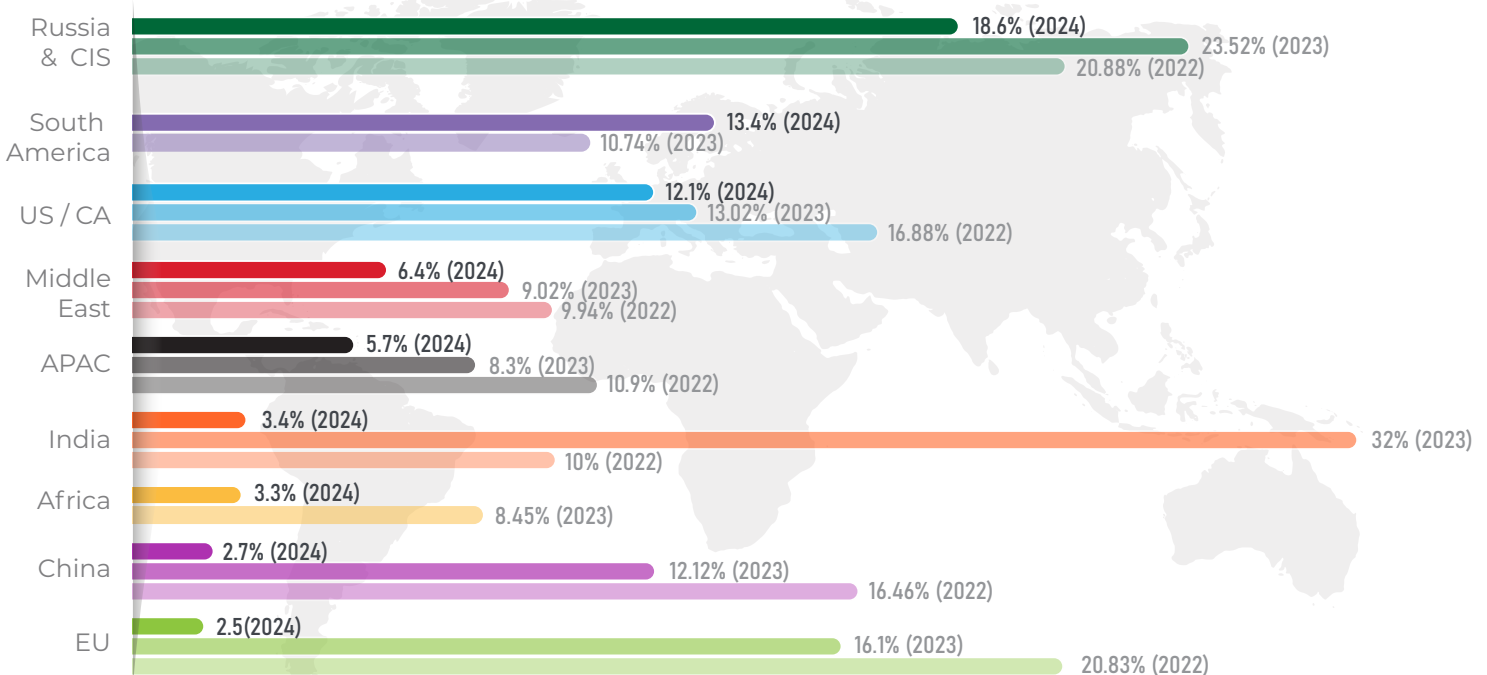


Web Ad Fraud in 2024

Geo-distribution

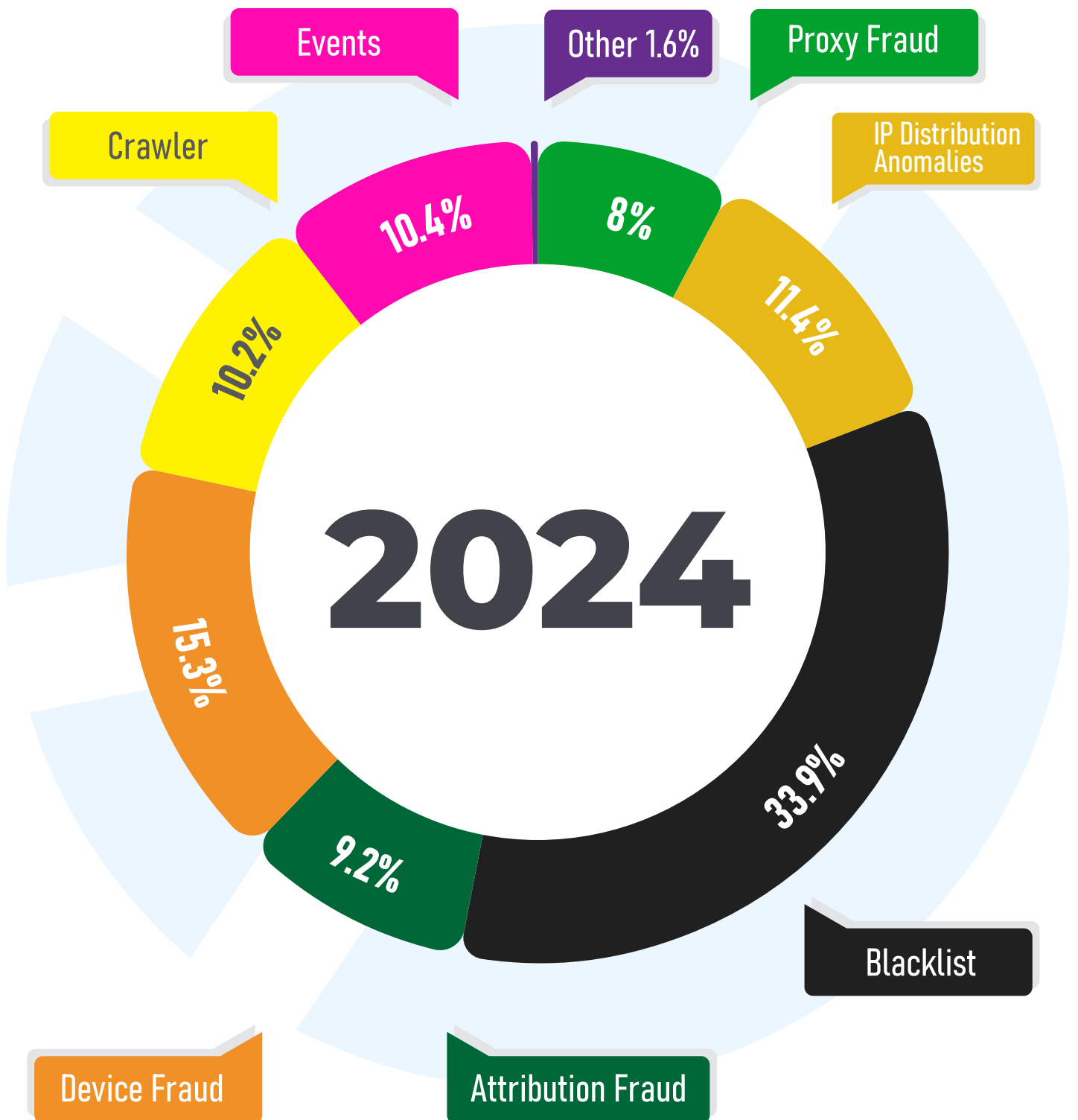


2024 / 2023 / 2022



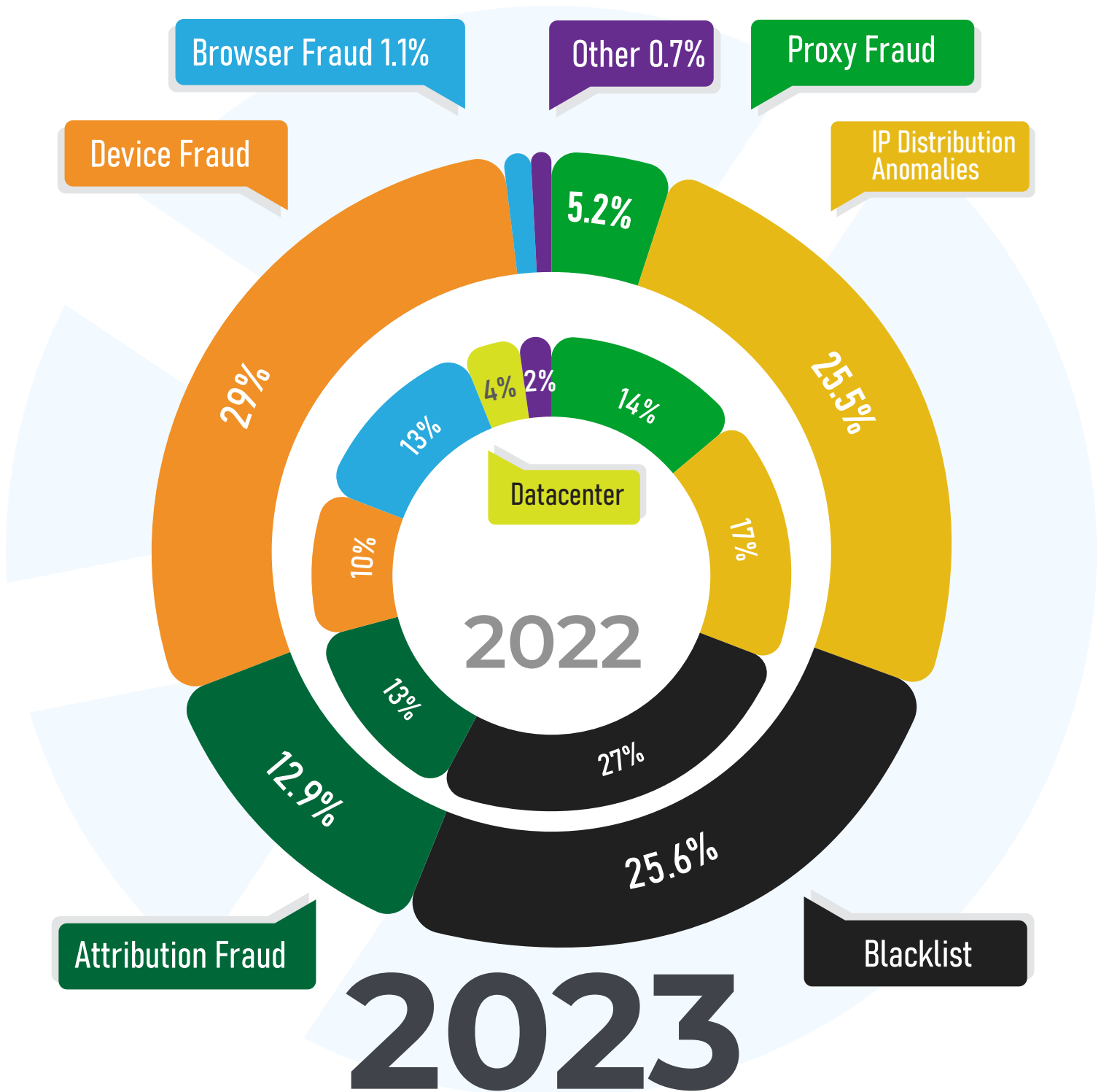
Web Ad Fraud in 2024

Distribution by the Main Detected Fraud Categories



Web Ad Fraud in 2024 vs 2023/2022

Distribution by the Main Detected Fraud Categories



Outcomes & Trends from 2024

The digital advertising world of 2024 brings a clear, sobering truth: ad fraud not only remains but has become an even more dangerous threat. Fraudulent traffic reached a staggering 40.76% of global traffic, a view-through of over 260 billion adverse impacts, up from 37.71% in 2023 — the digital landscape is still bleeding resources.

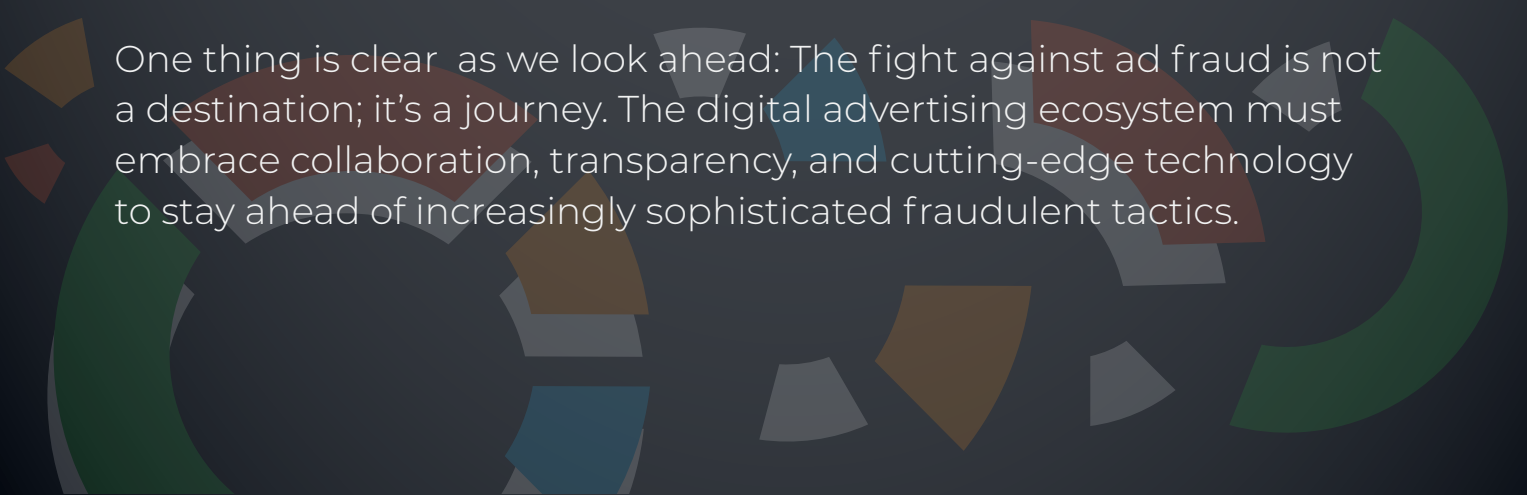
Ad fraud accounted for an estimated global loss of over \$140 billion in 2024, making it clear that effective and evolving fraud prevention is imperative for the industry to move forward. Mobile platforms continue to be most vulnerable, with the Android platform ahead at a 42.67% fraud rate versus the iOS platform, which followed up at 36.73%.

Geographically, the fraud landscape remains complex. China, the EU, and Russia & CIS regions emerged as the top three hotspots for fraudulent activities, with mobile markets showing particularly high-risk profiles. The most fraud-prone app categories further highlight the depth of the challenge: Finance apps on Android (55.9%) and iOS (61.6%) stand out as prime targets for fraudsters.

The tactics may continue to evolve — where Blacklist (28.84%), Events (22.75%), and IP Distribution Anomalies (12.85%) take the lead — but the story is the same: ad fraud is a living, breathing threat, and response must be as well.

At FraudScore, we understand that these figures are not just numbers on a page but substantial financial threats faced by companies across the globe. We report on these trends and help build ever more advanced detection and prevention systems.

One thing is clear as we look ahead: The fight against ad fraud is not a destination; it's a journey. The digital advertising ecosystem must embrace collaboration, transparency, and cutting-edge technology to stay ahead of increasingly sophisticated fraudulent tactics.



Main Fraud Categories

by Fraudscore

FraudScore is known for its know-how approach to traffic evaluation and fraud categories division in detected malicious schemes.

Here you can find the definition for the majority of general ad fraud categories that are used in FraudScore reports and statistics.

Fake Attribution

All the suspicious activities that are possible to be fraud in attribution:

- Clickspamming - App installs previously attributed to clicked ads were discovered to be user-generated app installs randomly claimed by ad networks by spamming the fingerprinting algorithms.
- Cookie stuffing - the process by which a client is provided with cookies from other domains as if the user had visited those other domains. Taking ad tags from a publisher's site and putting them on to another site without the publisher knowledge.
- Click injection(Android only) - Android is uniquely vulnerable to click injection fraud, in which an ad network takes credit for organic app installs.

Crawler

- Search engines and other automatic crawlers.

Device Anomalies

All the abnormal device parameters are signs that there is "device fraud":

- Fake device IDs (user agent, IDFA/Android ID, MAC address, etc.) and their combinations.
- Device emulators.
- Hijacked device where a user is present and additional HTML or ad calls are made independently of the content being requested by the user IP (all the violations identified by the IP address in conjunction with other parameters of conversion).

Datacenter IP

- A fraud reason category that identifies servers which means that there are no real human users. Traffic originates from servers in data-centers or known cloud platform providers, rather than residential or corporate networks and where the ad is not rendered on a user's device.

Main Fraud Categories

by Fraudscore

IP Distribution Anomalies

Abnormalities that are connected with IP addresses.

- Multiple conversions from the same IP
- Multiple conversions from the same IP subnet etc.

Operating System (OS) Anomalies

- Anomalies within an Operating system that are fraudulent: abnormal device distribution within traffic (device models, browser versions, operating system, etc.)

Proxy Fraud

All the violations identified by the IP address in conjunction with other parameters of conversion are processed as symptoms for PROXY violations:

- Traffic that is routed through an intermediary proxy device or network where the ad is rendered on a user's device where there is a real human user
- IPs that are associated with known Botnets and Adware
- Users are actively hiding their identity or making conversions from an unwanted GEO

Events

- Group of parameters that help identify fraudulent conversions based on in-app event data. For example, conversions made by users who did not continue working in the app after the target event.

BlackList

- Suspicious parameters that are detected when an IP is included in fraudulent sources blacklists. Also, this might occur with dynamic IPs when there is still a correlation with fraudulent activities.

Other

- All possible anomalies that are detected by FraudScore and are a clear symptom of fraud. For instance, suspicious traffic sources, browser anomalies and never existing versions, etc.

Contact us for a free trial:
sales@fraudscore.mobi

FraudScore

the independent
antifraud solution

This report does not estimate all the global online advertising traffic and is based on data from traffic processed by the FraudScore platform in 2024, 2023 and 2022. The report highlights figures and statistics based on FraudScore data and hasn't been reviewed by a third party. FraudScore continues to improve its methods of traffic evaluation and is open to answering questions and inquiries about the report.

