Ad Fraud Report

by FraudScore

2025

Compared to 2024 and 2023

Trends Outcomes & Aftermath

Introduction

2025 represents the highest level of ad fraud observed by FraudScore to date. According to FraudScore's analysis, **47.40% of all analyzed advertising traffic in 2025 was classified as fraudulent,** exceeding results recorded in previous years.

This report is based on aggregated mobile and web traffic data analyzed by FraudScore across multiple advertising models, platforms, app categories, and geographic regions. The analysis covers monthly fraud distribution, regional exposure, dominant fraud categories, and platform-specific characteristics for Android and iOS traffic.

The purpose of this report is to provide a structured, quantitative overview of how ad fraud levels and composition evolved throughout 2025, and how these changes compare to prior years. All figures presented are derived from FraudScore's proprietary fraud detection methodology and reflect observed traffic patterns during the reporting period.

In this Report, FraudScore presents:

- Annual and monthly fraud rates and year-over-year comparisons
- Geographic distribution of fraudulent traffic
- Distribution of major detected fraud categories
- Mobile VS web fraud dynamics
- Android and iOS platform-specific insights, including app category exposure

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.

Methodological approach

FraudScore's analysis is based on the evaluation of **all incoming traffic without preliminary exclusions** by baseline invalidity criteria. This approach allows for a comprehensive view of traffic quality and reflects real-world campaign exposure rather than pre-filtered datasets.

In its methodology, FraudScore applies detection principles aligned with commonly accepted industry definitions of **General Invalid Traffic (GIVT).** These include the identification of known invalid traffic sources such as:

- datacenter-generated traffic
- crawlers, parsers, and other automated systems
- excessive or abnormal activity patterns

The primary focus of FraudScore's analysis is traffic associated with **performance-based advertising models,** predominantly **CPA-driven campaigns.**

For **Sophisticated Invalid Traffic (SIVT),** FraudScore evaluates **post-install and post-action user behavior,** with particular attention to anomalies in user event patterns. Such anomalies are identified and classified within the **Events-related risk group,** enabling the detection of complex and behavior-based fraud that occurs beyond the initial attribution stage.

2025 in facts

47.4%

of all analyzed traffic in 2025 was classified as **fraudulent**

2025

recorded the highest fraud rate observed by FraudScore to date

Mobile traffic

remained the primary contributor to overall fraud volume

Fraud activity

intensified significantly in the second half of the year

Sustained fraud peaks

indicate scalable and organized fraud operations

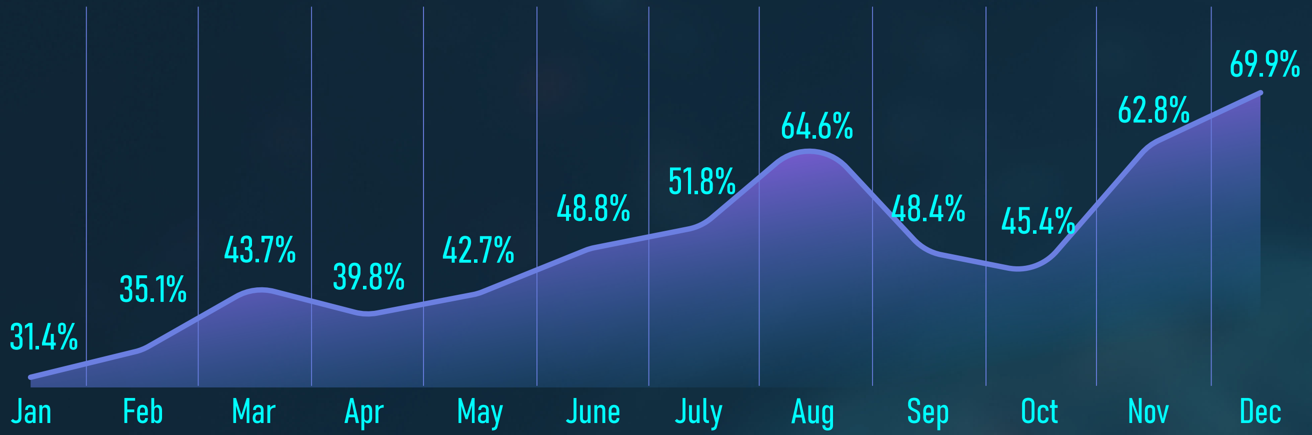
Monthly

fraud volatility reached unprecedented levels

Ad Fraud in 2025

2025 total 47.4%

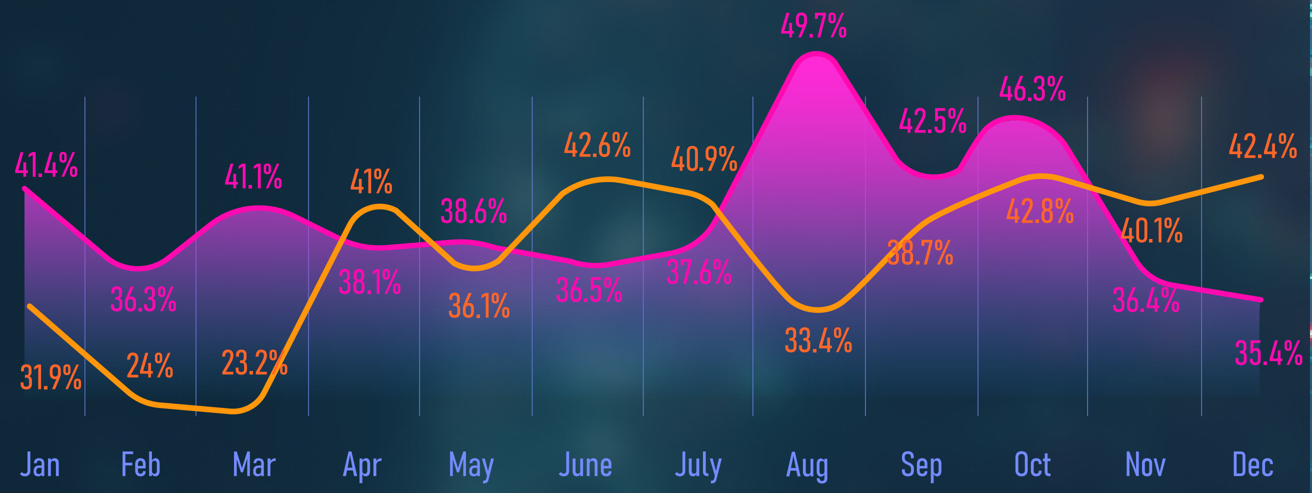
All processed traffic



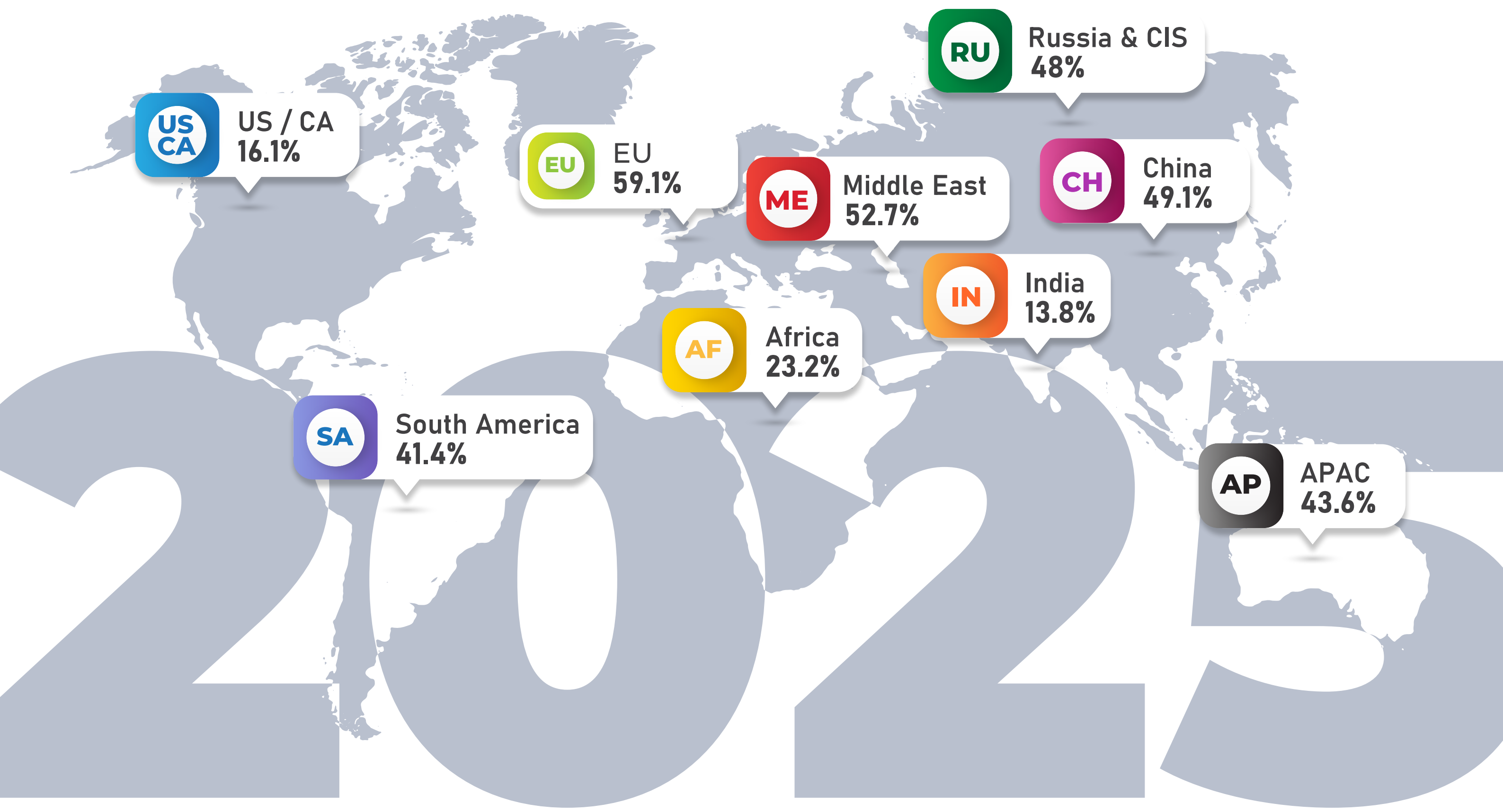
2024 total 40.76%

2023 total 37.71%

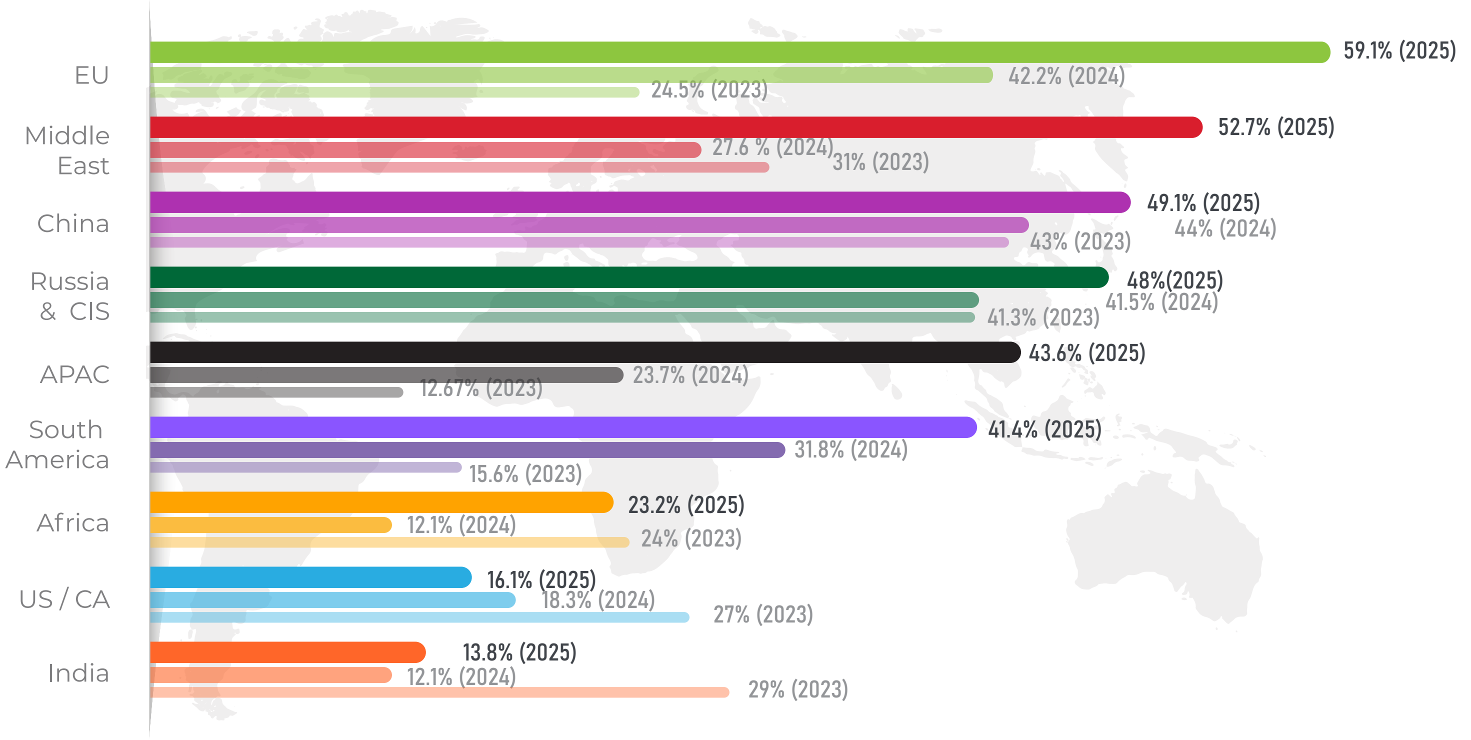
All processed traffic



2025 Geo-distribution

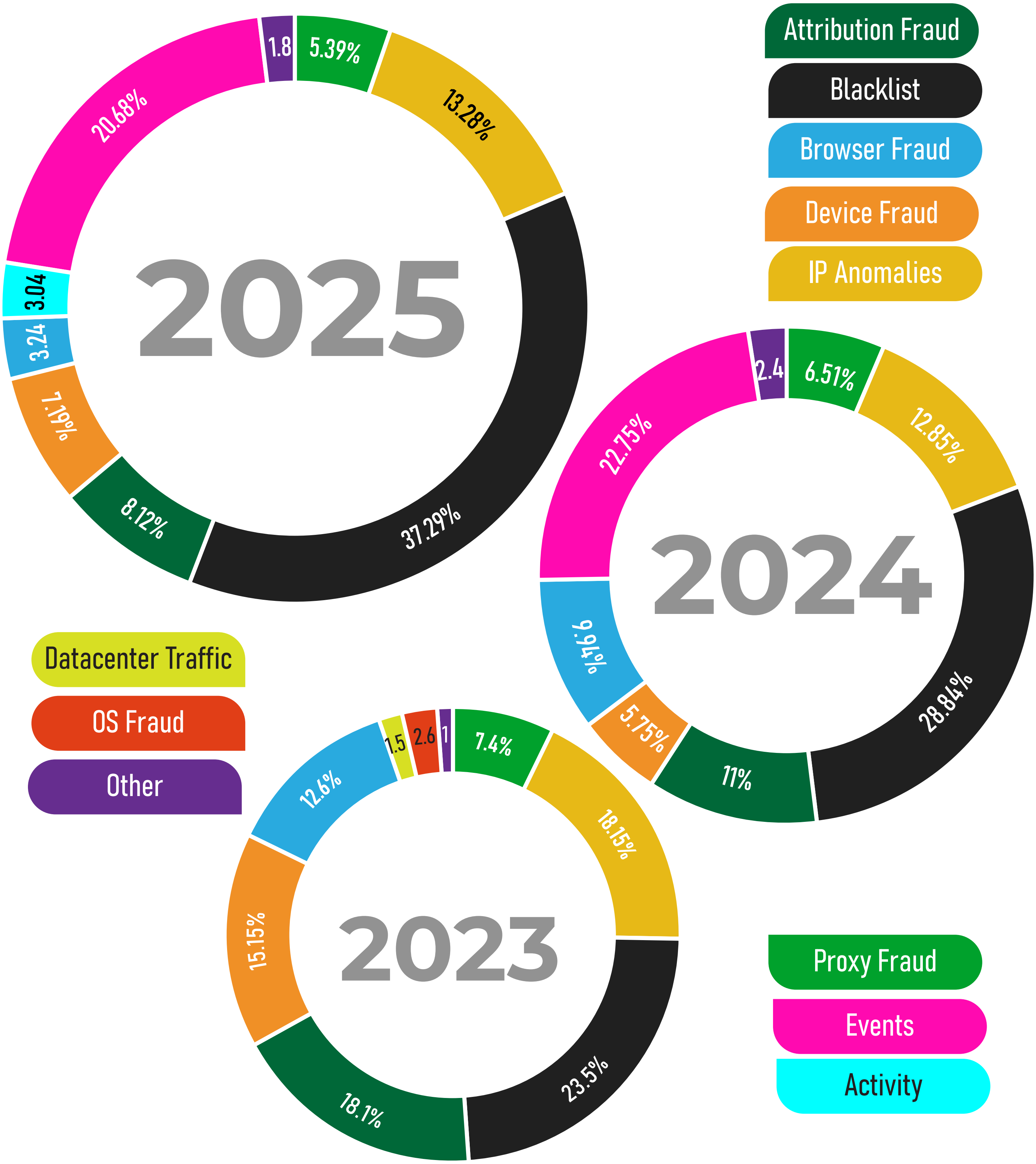


2025 / 2024 / 2023



Main Fraud Categories

Distribution Ad Fraud by the Main Detected Fraud Categories

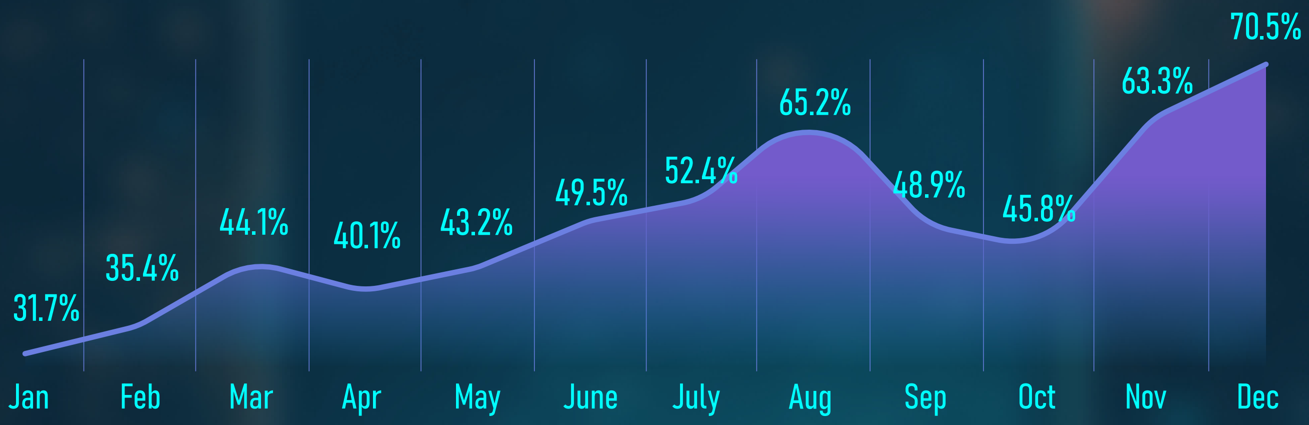


Mobile Ad Fraud in 2025

2025 total 47.77%

Mobile

% of ad fraud in global mobile traffic

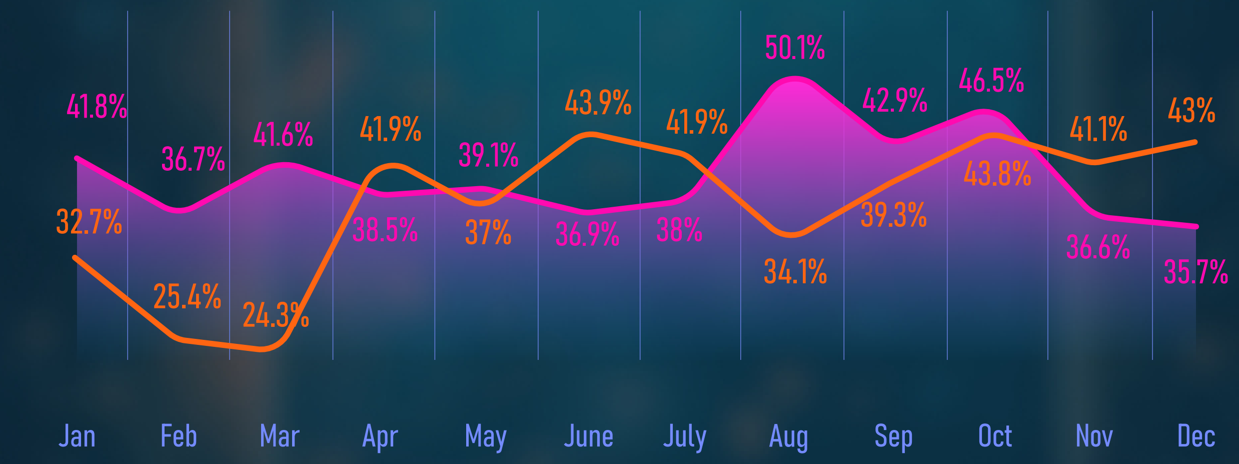


2024 total 41.09%

2023 total 38.65%

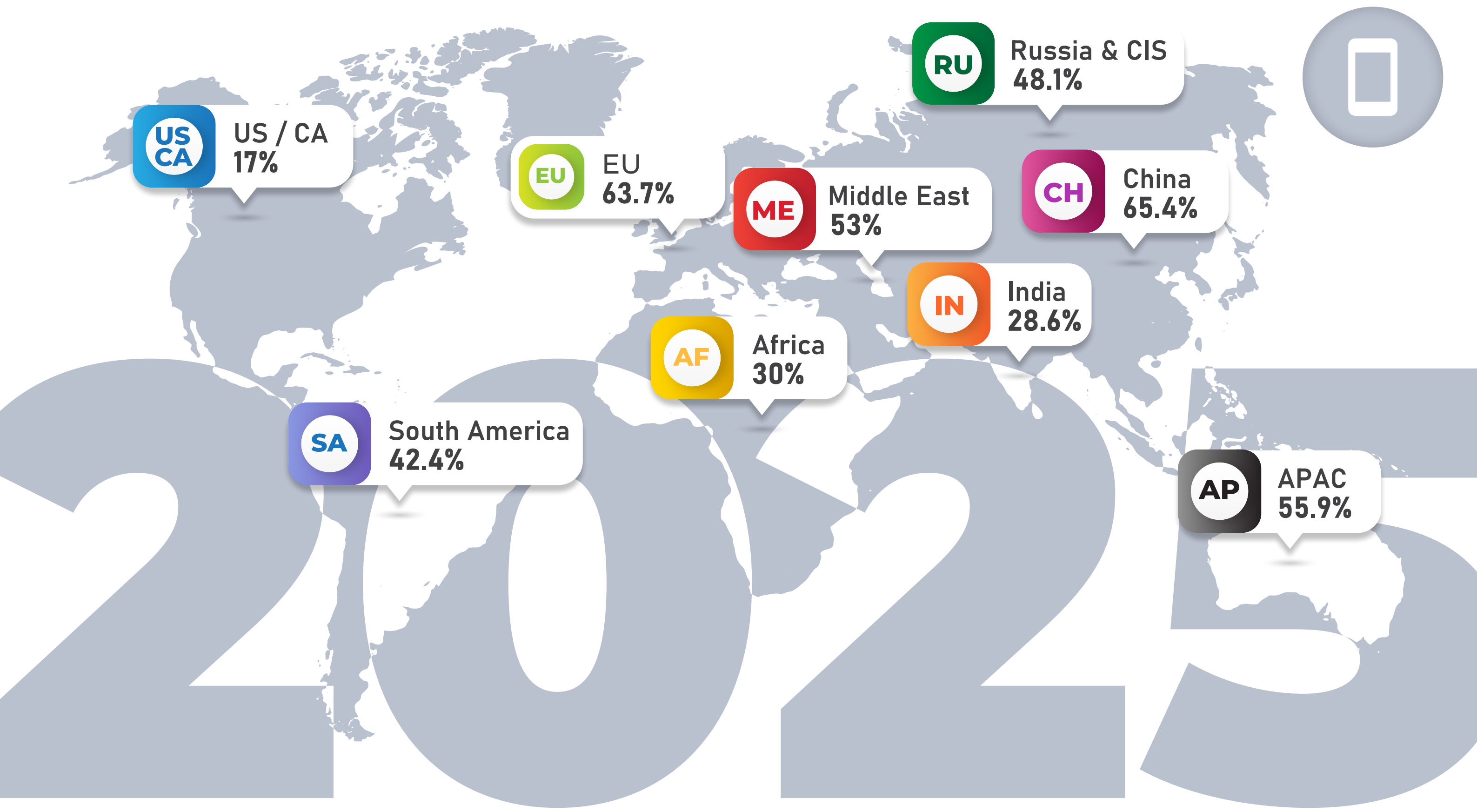
Mobile

% of ad fraud in global mobile traffic

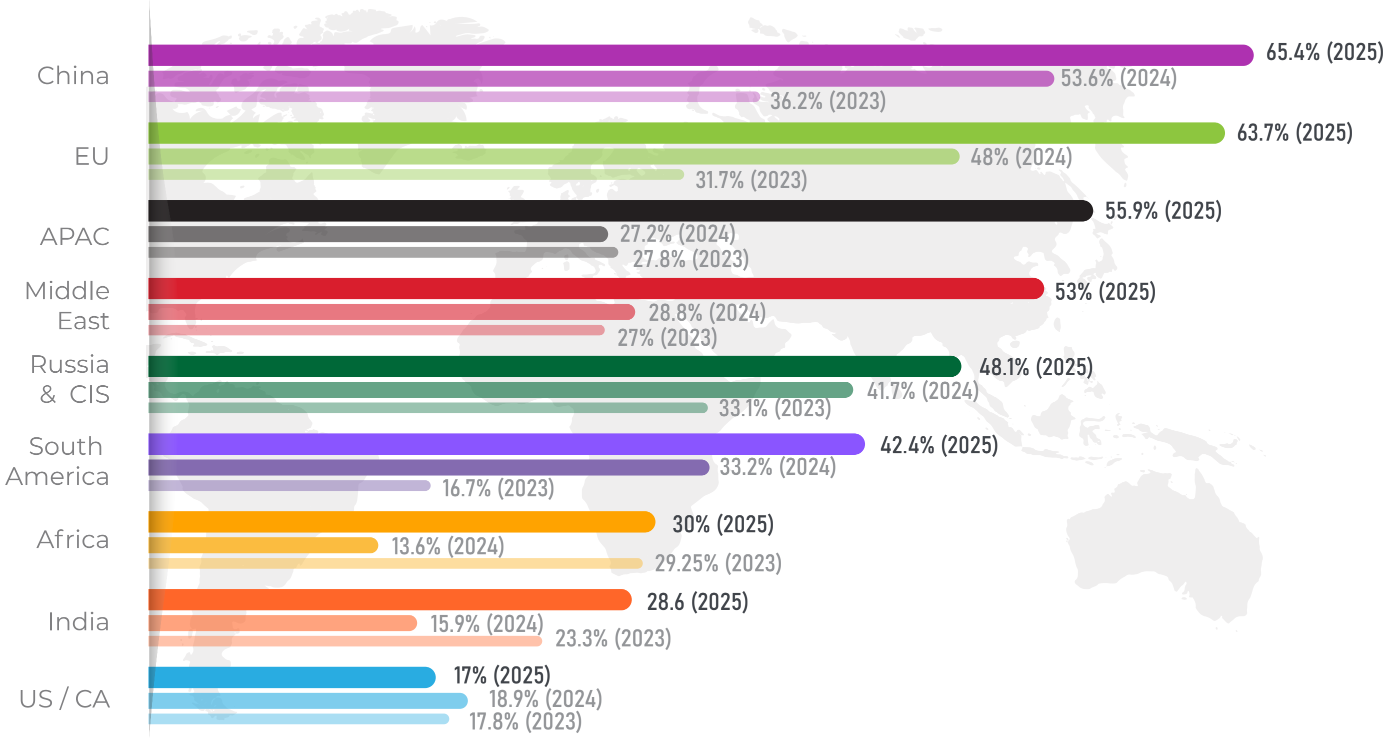


Mobile Ad Fraud in 2025

Geo-distribution

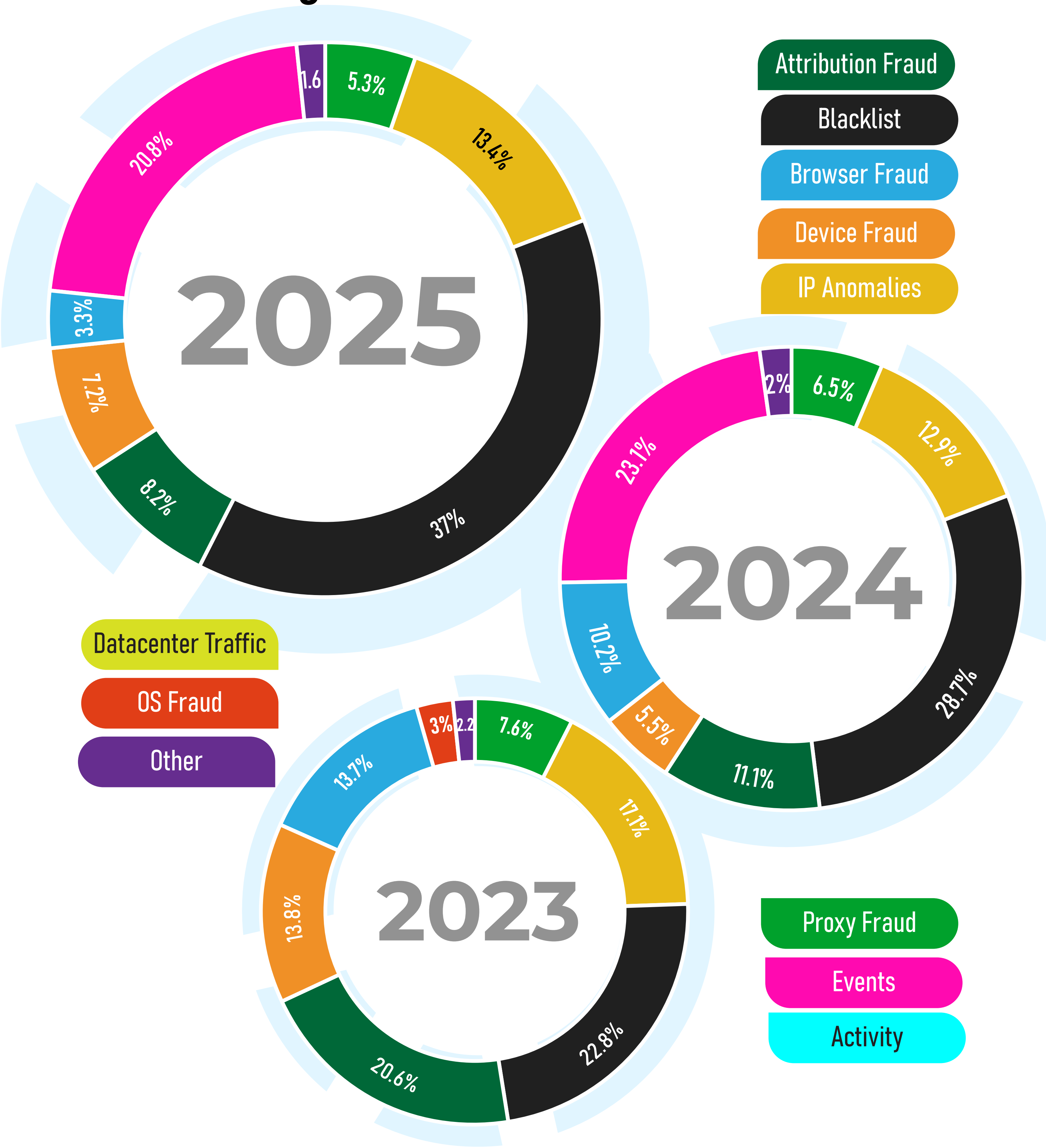


2025 / 2024 / 2023



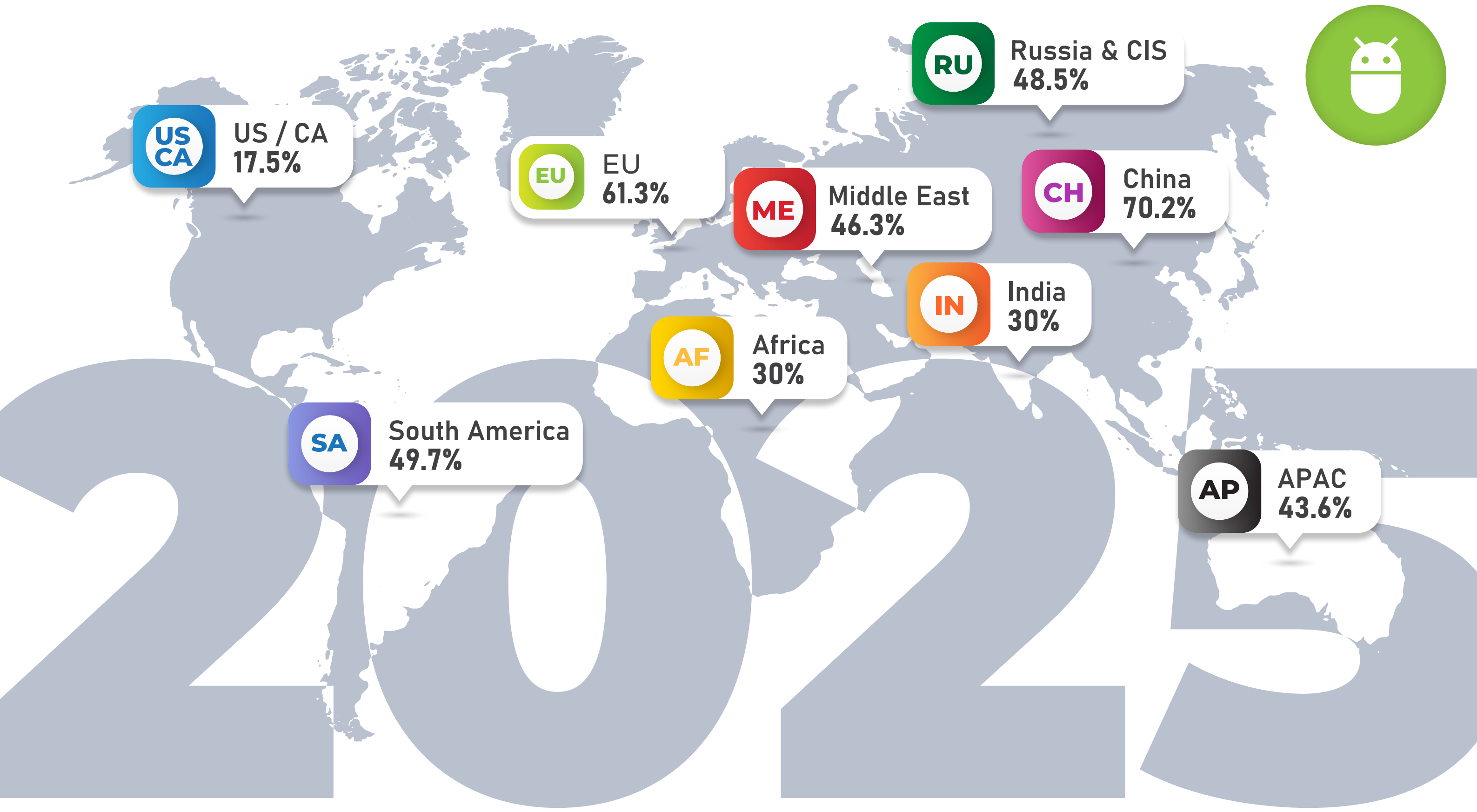
Mobile Ad Fraud in 2025

Distribution by the Main Detected Fraud Categories



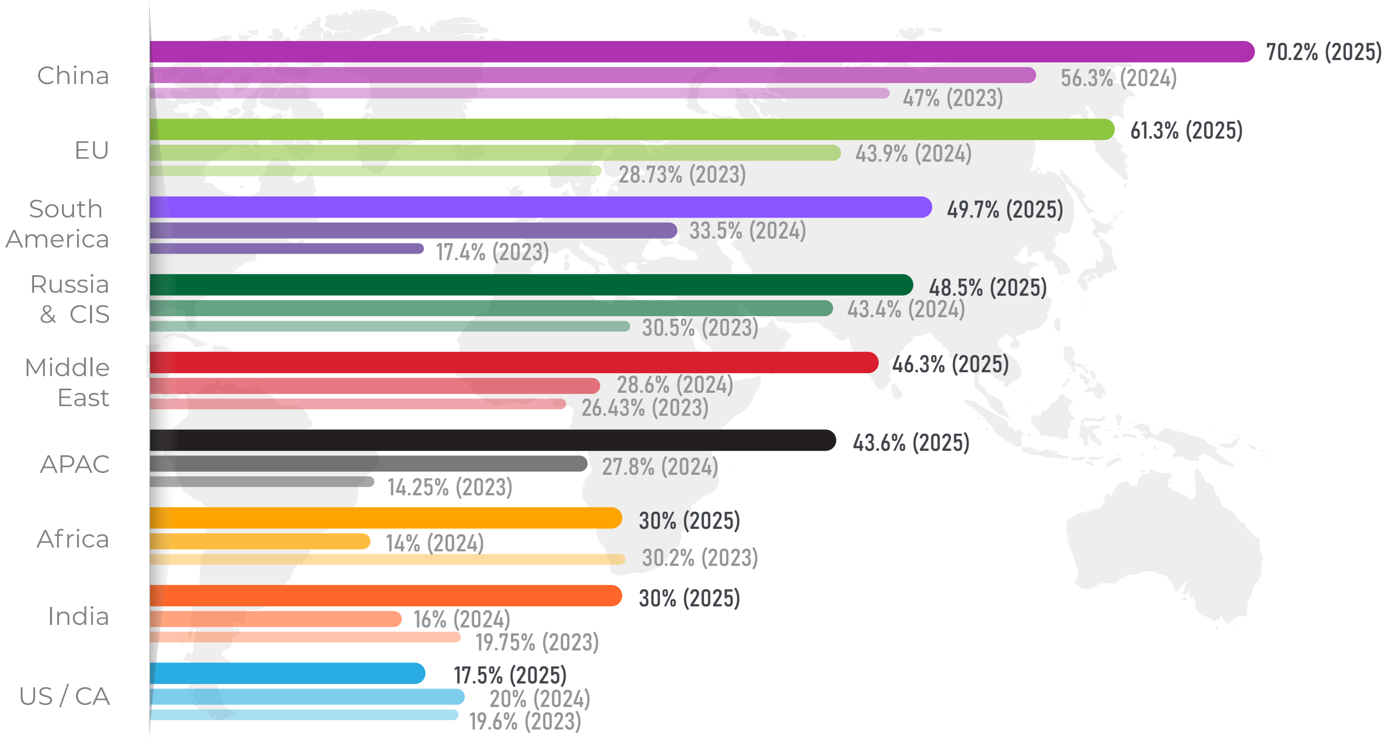
Andriod Ad Fraud in 2025

Geo-distribution

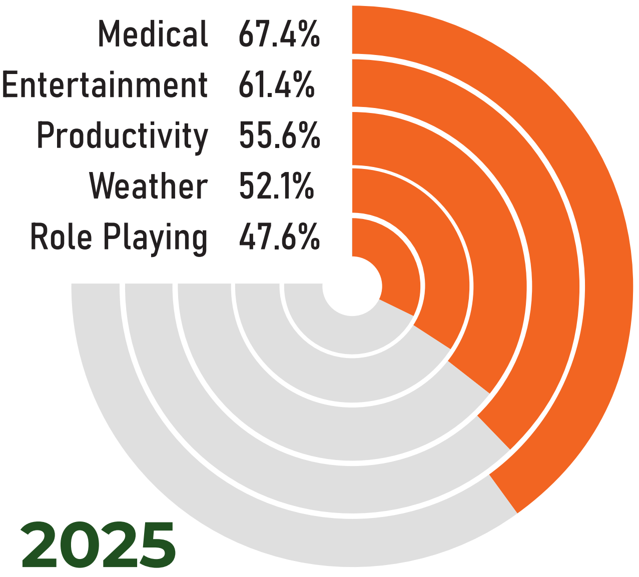


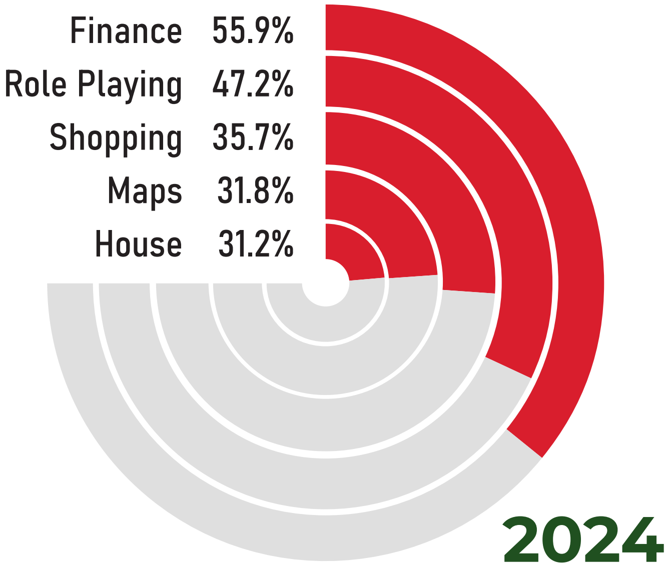
2025 / **2024** / **2023**

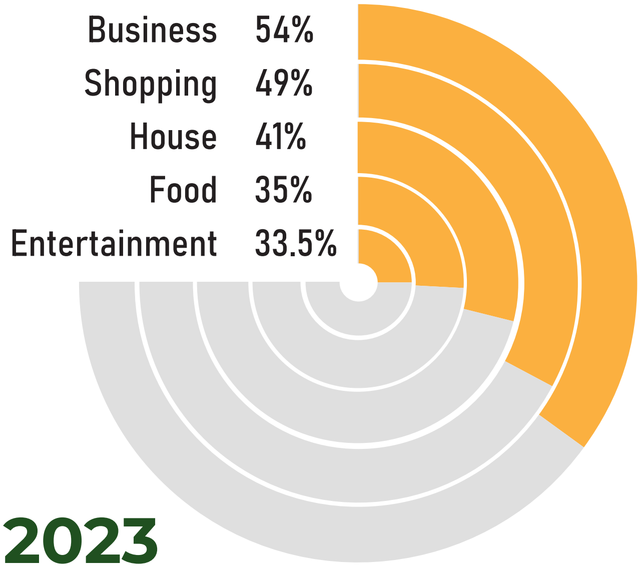
total amount 33.1% | total amount 42.7% | total amount 40.39%



The Most Fraud-prone App Categories on Android: comparison







55.6%
Productivity

67.4%
Medical

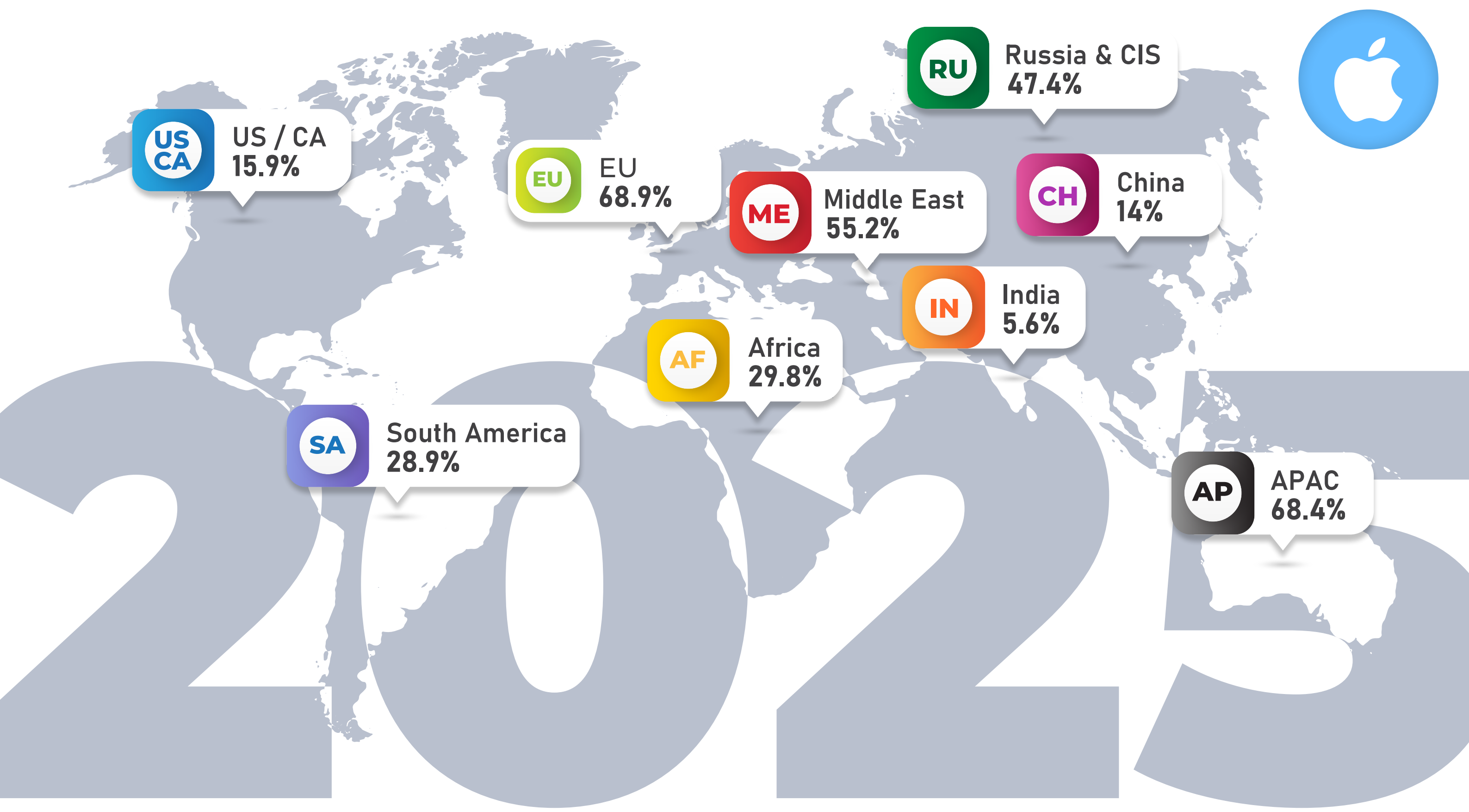
61.4%
Entertainment

52.1%
Weather

47.6%
Role Playing

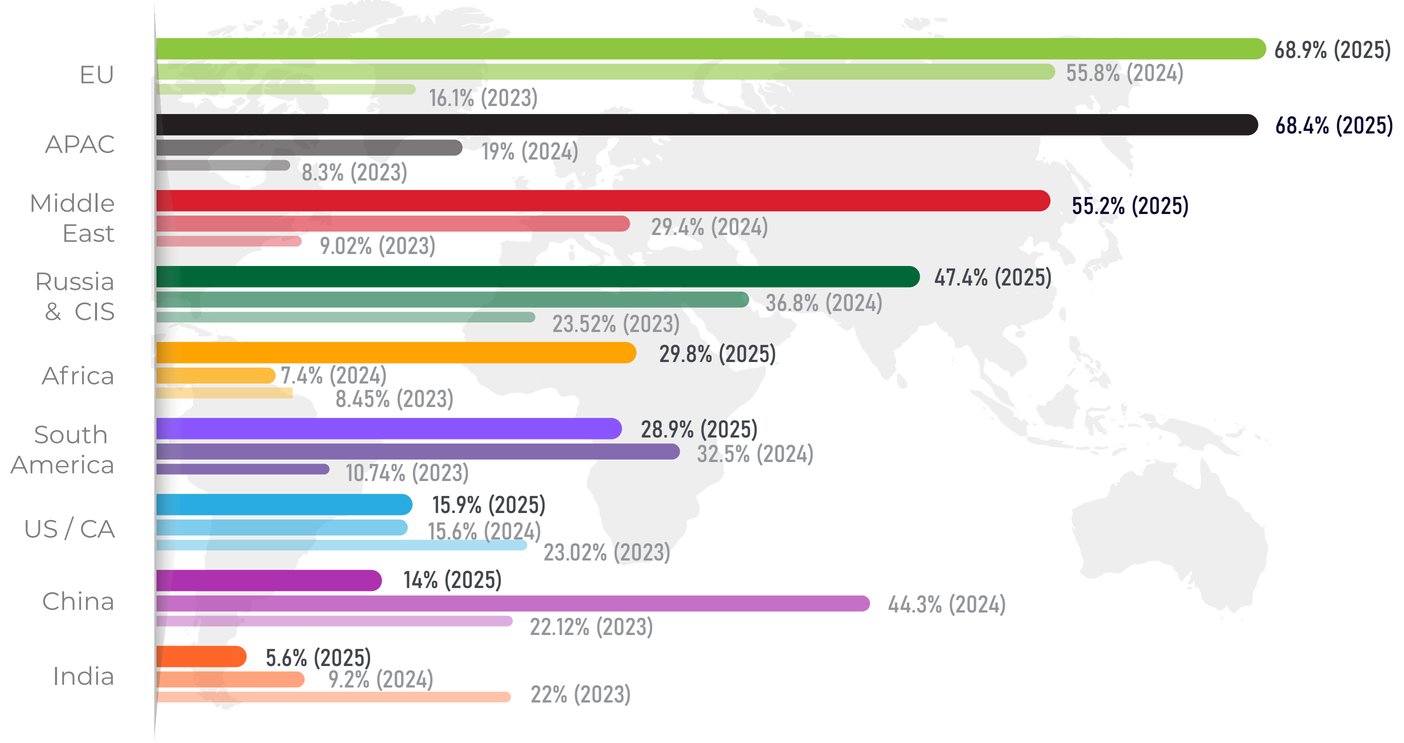
iOS Ad Fraud in 2025

Geo-distribution

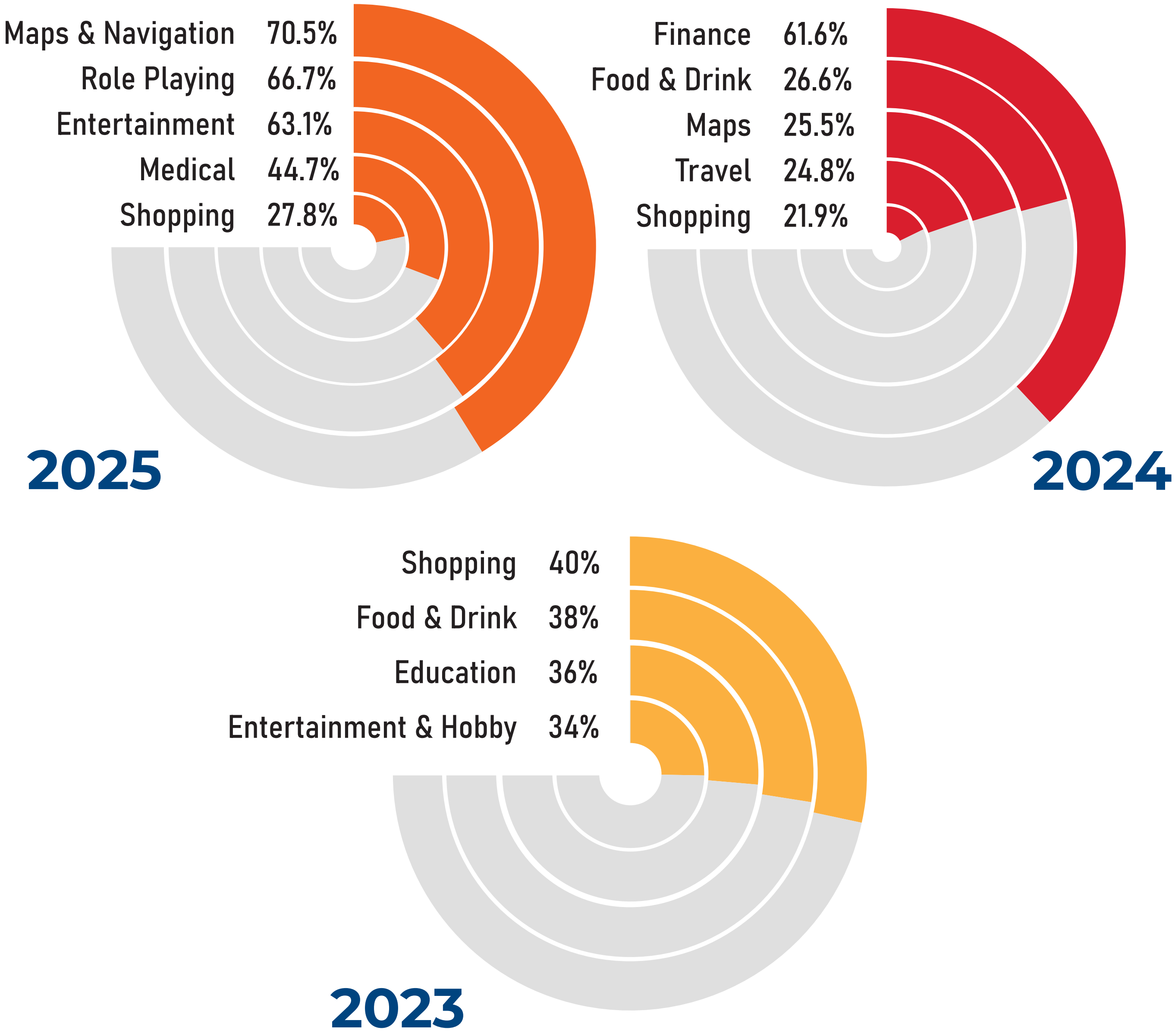


2025 / 2024 / 2023

total amount 29.8% — total amount 34.7% — total amount 26.54%



The Most Fraud-prone App Categories on iOS: comparison



70.5%
Maps & Navigation

66.7%
Role Playing

63.1%
Entertainment

44.7%
Medical

27.8%
Shopping

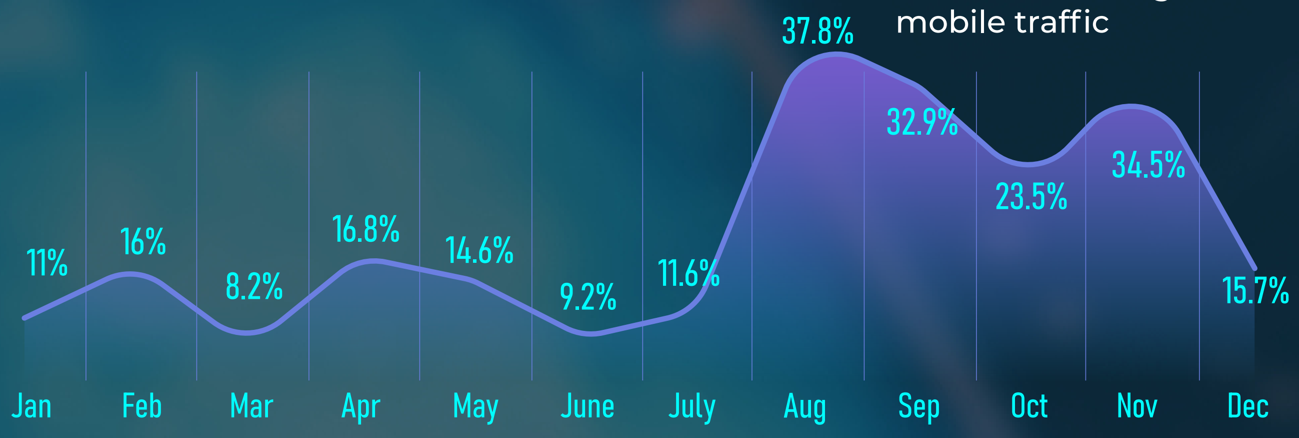
2025

Web Ad Fraud in 2025

2025 total 19.45%

Web

% of ad fraud in global mobile traffic

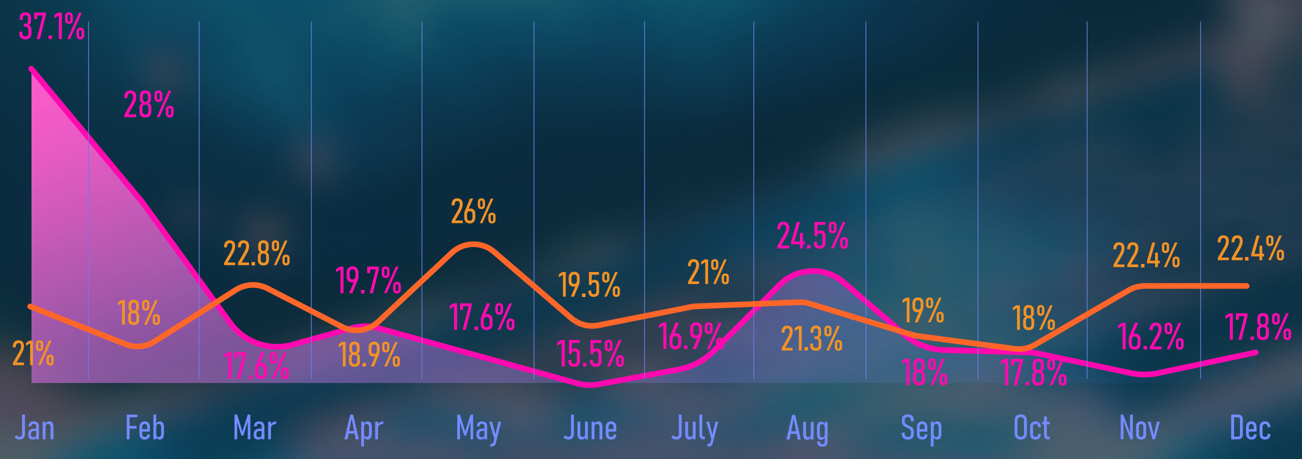


2024 total 21.03%

2023 total 20.82%

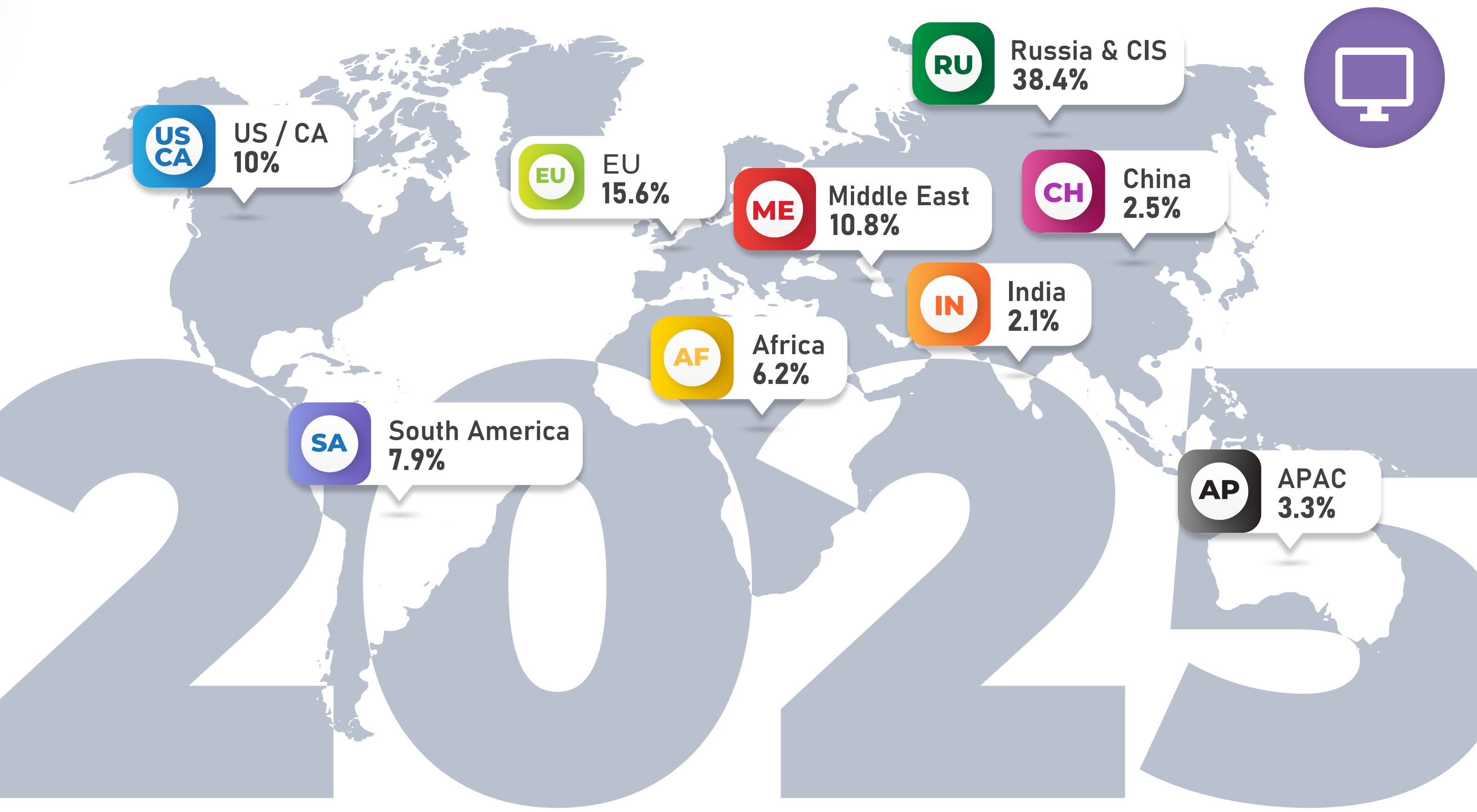
Web

% of ad fraud in global mobile traffic

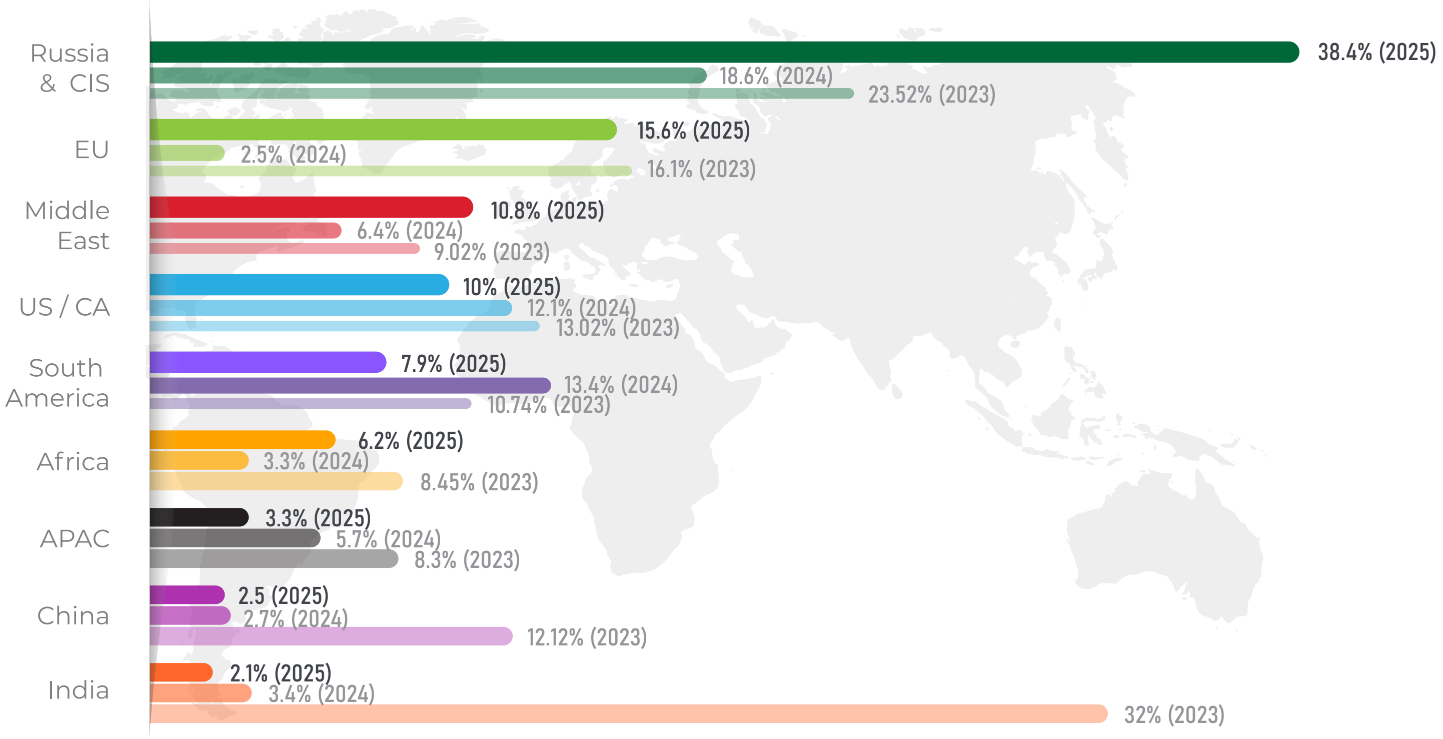


Web Ad Fraud in 2025

Geo-distribution

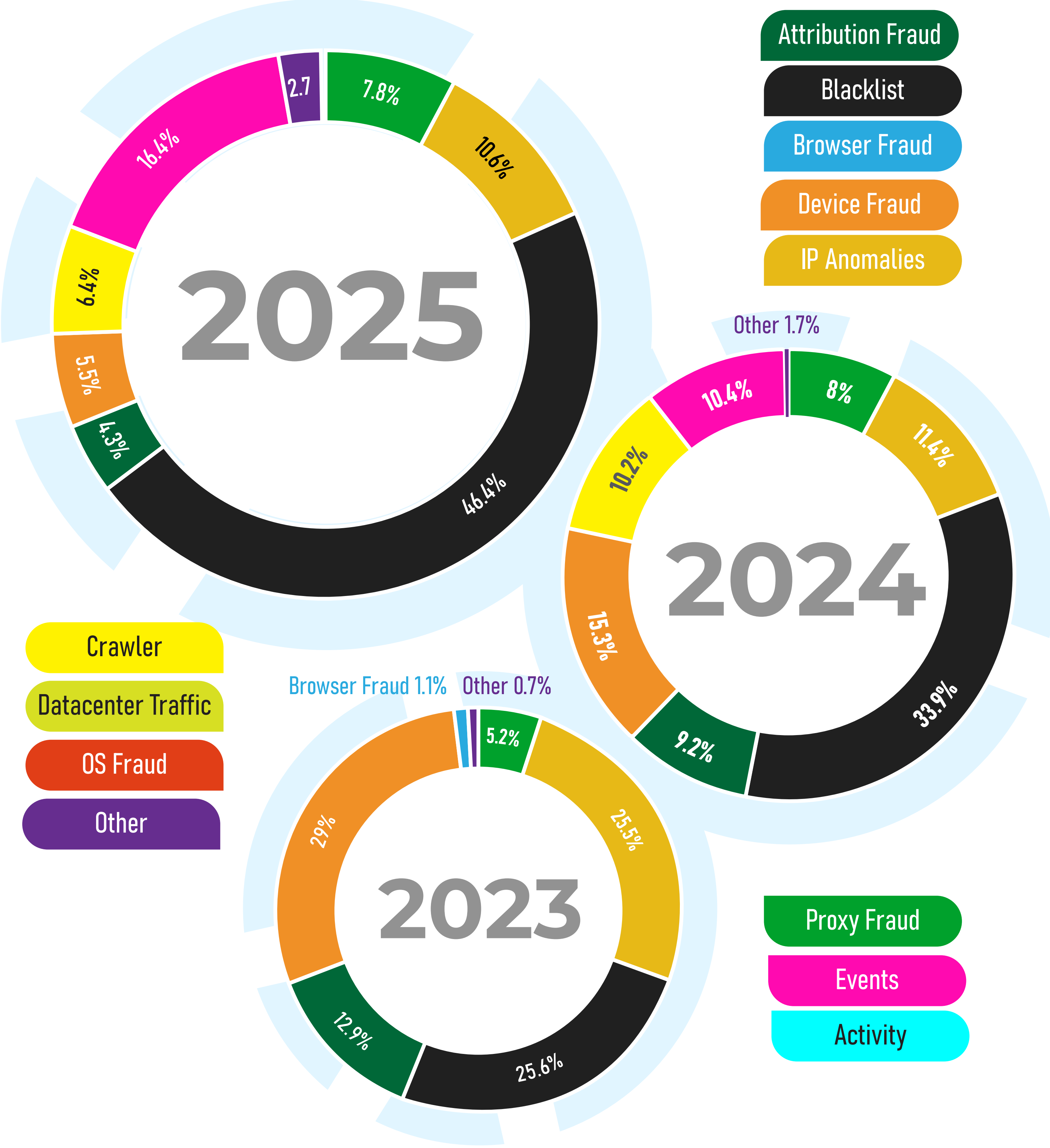


2025 / 2024 / 2023



Web Ad Fraud in 2025

Distribution by the Main Detected Fraud Categories



Outcomes & Trends from 2025

Data from 2025 indicates a continued escalation of ad fraud activity, with overall fraud levels increasing to 47.40%, compared to 40.76% in 2024. The increase was not uniform throughout the year and was largely driven by the second half of 2025.

From June onward, monthly fraud rates exceeded historical averages and remained elevated through year-end, reaching 64.6% in August and 69.9% in December. Unlike prior years, these elevated levels persisted across consecutive months, indicating repeatable and stable traffic generation rather than isolated fraud bursts.

Mobile traffic remained the dominant contributor to fraudulent volume. While overall mobile fraud growth followed the general market trend, platform-specific patterns differed. Android traffic exhibited broad regional exposure with consistently high fraud levels across most regions, while iOS fraud showed stronger concentration within specific app categories.

Structurally, 2025 was marked by a shift in dominant fraud methods. Blacklist-related fraud increased significantly, accounting for over 37% of all detected fraud, while Events fraud and IP Distribution Anomalies remained key contributors. The relative share of attribution fraud declined compared to previous years, suggesting adjustments in fraud tactics rather than an overall reduction in fraudulent activity.

Regionally, fraud exposure intensified across multiple markets. The EU, China, APAC, and the Middle East demonstrated strong year-over-year growth, while Russia & CIS continued to exhibit consistently high fraud levels across both mobile and web environments.

Overall, 2025 data points to a pattern of sustained fraud activity, increased method concentration, and stronger regional clustering, highlighting the importance of continuous monitoring and granular traffic analysis.

Main Fraud Categories
by FraudScore

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

The following section provides definitions of the majority of general ad fraud categories used in FraudScore reports and statistics.

Fake Attribution

All suspicious activities that may indicate attribution fraud:

- Clickspamming - App installs previously attributed to clicked ads were discovered to be user-generated app installs randomly claimed by ad networks through fingerprinting spam.
- 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 onto another site without the publisher's 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

Abnormal device parameters that indicate device fraud include:

- Fake device IDs (user agent, IDFA/Android ID, MAC address, etc.) and their combinations.
- Device emulators.
- Hijacked devices occur when a legitimate user is present but additional HTML or ad calls are generated independently of the content requested by the user. All such violations are identified using the IP address in conjunction with other conversion parameters.

Datacenter IP

- A fraud reason category that identifies server-originated traffic, meaning 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 routed through an intermediary proxy device or network, even though the ad is ultimately rendered on a real user's device.
- IPs that are associated with known Botnets and Adware.
- Users are actively hiding their identity or making conversions from an unwanted GEO

Events

- A group of parameters used to 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 non-existent versions, etc.

www.fraudscore.ai

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.