

ADS SAFETY

# Q1 2026

## Ads Safety Report

How PropellerAds Policy & Security teams stay ahead of evolving ad fraud — key insights on campaign rejections, suspension patterns, and emerging high-risk geographic markets.

**36,085**

Campaigns rejected  
in Q1 2026

**~48%**

Adult content —  
top rejection category

**68.1%**

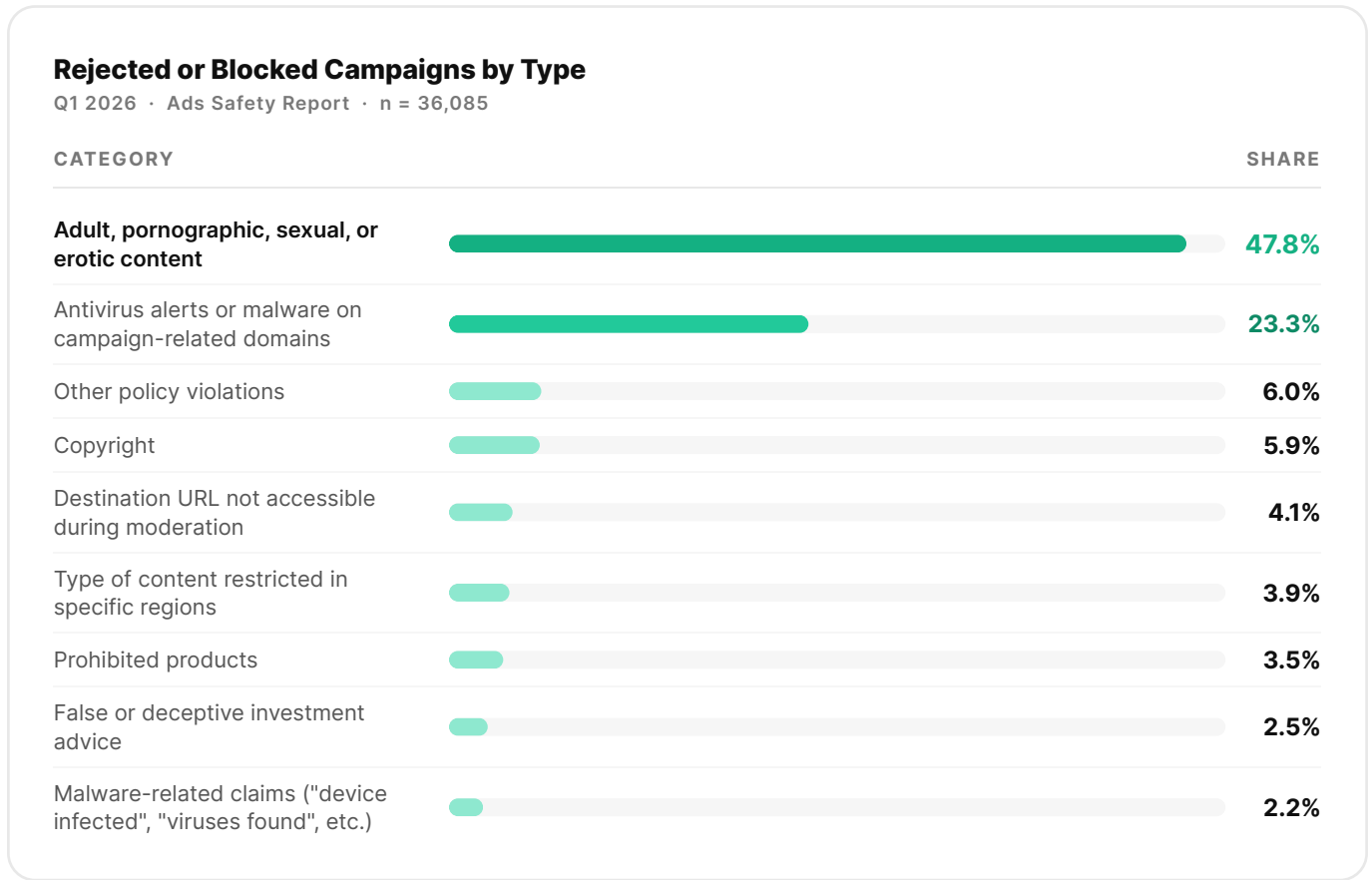
Cloaking — #1  
suspension reason

PropellerAds Policy and Security teams continuously monitor evolving fraud patterns across our ecosystem, keeping a close eye on new tactics and emerging risks. As part of our commitment to transparency, we regularly publish open reports that highlight key trends, violations, and areas of concern.

In this report, we break down the latest data on rejected or blocked campaigns, uncover the most common abuse patterns, and highlight high-risk GEOs where fraudulent activity is most concentrated. These insights help us not only strengthen our moderation processes but also provide advertisers with a clearer understanding of the current risk landscape.

# Rejected or Blocked Campaigns By Type

In Q1 2026, **36,085 ad campaigns** were rejected for non-compliance with platform rules and terms and conditions.



**47.8%**  
Adult content — dominant violation, wider gap vs. 2025 report.

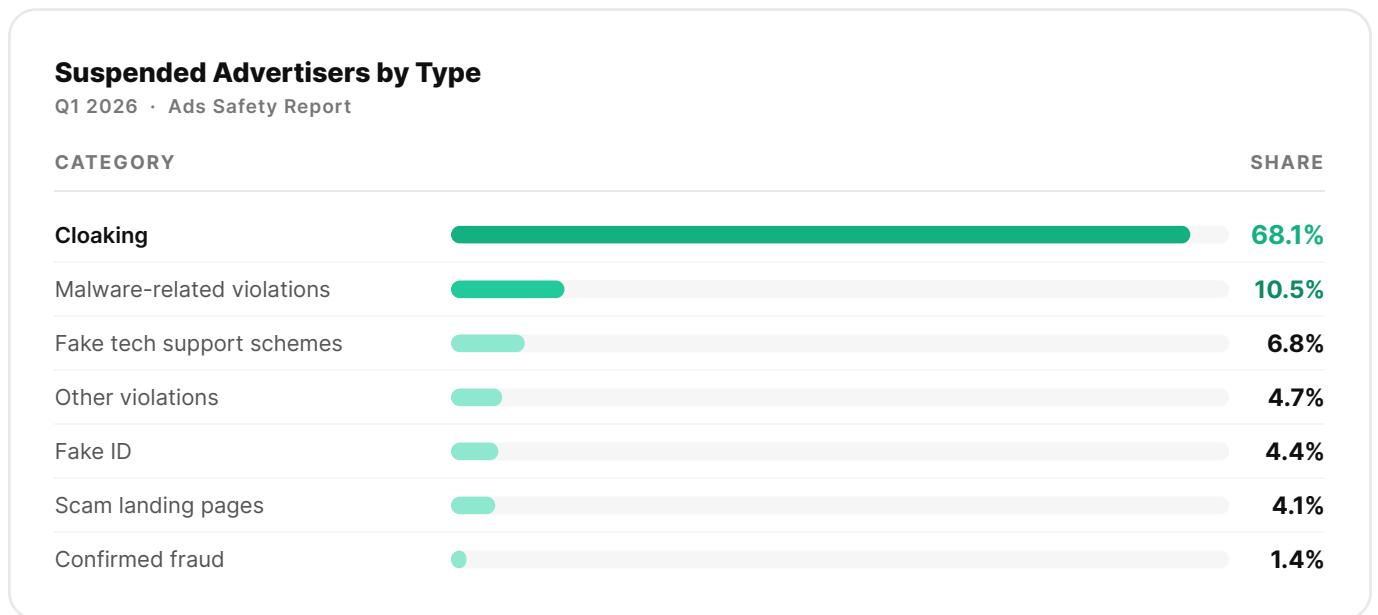
**23.3%**  
Malware & unsafe landing pages — persistent secondary concern.

Almost half of all rejections (~48%) are tied to **adult content**, making it the dominant policy violation by a wide margin. This aligns with the 2025 report, where adult-related violations were also the leading category — the current data shows an even clearer dominance.

The second-largest share (23%) comes from **malware-related issues**, showing that unsafe or compromised landing pages remain a major concern. All other categories are significantly smaller and reflect external complaints and specific compliance issues rather than large-scale abuse.

# Suspended Advertisers By Type

The vast majority of account suspensions are driven by **cloaking (nearly 70%)**, clearly indicating that the main issue is not isolated violations — it is systematic attempts to bypass moderation.



**Cloaking is not just a policy issue — it's an infrastructure problem.** Fraudsters build complex systems to hide real landing pages from moderators. Malware, scam pages, and fake IDs are largely **layers built on top of cloaking schemes**, not independent violations.

**68.1%**  
Cloaking — core mechanism driving the majority of all suspensions.

**10.5%**  
Malware — most stable secondary category; persistent across quarters.

Compared to the 2025 report, this indicates **continuity rather than a shift**: cloaking remains the core mechanism behind most violations. Malware continues to be one of the most stable secondary risk categories, reinforcing that unsafe landing pages remain a persistent issue rather than a temporary spike.

# High-Risk GEOs

Fraudulent activity is not evenly distributed. Three geographic clusters account for the majority of policy violations and suspension triggers identified in Q1 2026.



## Tier-1 Markets

HIGH-INVESTMENT FRAUD

Higher advertiser payouts (CPC/CPA) make these markets economically attractive for **high-investment fraud**, such as cloaking and malware distribution. The strong monetization potential justifies building more complex infrastructure to bypass stricter moderation systems.

US · UK · CA · AU · DE

Cloaking

Malware Distribution

High CPC / CPA



## LATAM

HIGH-VOLUME FRAUD

Lower traffic costs combined with large, growing audiences enable **high-volume fraud models**. These markets are often exploited to scale misleading creatives and scam flows. Strong demand for financial offers creates opportunities for fraudsters posing as trusted banks and services.

BR · MX · AR · CO

Financial Scams

Misleading Creatives

Low Traffic Cost



## Turkey (TR)

MIXED RISK PROFILE

Turkey presents a balanced mix of moderate traffic costs and strong conversion potential, making it a target for malicious actors — e.g., **misleading subscription flows or deceptive offers**. It sits between Tier-1 monetization efficiency and emerging market scale in terms of risk exposure.

TR

Subscription Fraud

Deceptive Offers

Prohibited Campaigns

**KATE SHMELEVA**

Head of Business Security, PropellerAds

*Tier-1 markets combine high payouts with strict regulations, making them a prime target for cloaking tactics. In Turkey, relatively low-cost traffic is often exploited to run prohibited campaigns, while in rapidly growing LATAM markets, strong demand for financial offers creates opportunities for fraudsters to imitate trusted banks and services to mislead users.*

## Our Commitment to Ads Ecosystem Safety

As fraud tactics continue to evolve, we remain committed to proactively identifying and addressing emerging threats across our ecosystem. By continuously refining our moderation processes and leveraging data-driven insights, we ensure a safer and more transparent environment for both advertisers and users.

We will continue to closely monitor key trends and regularly publish open reports to keep the market informed and help our partners navigate the changing risk landscape with confidence.



### Proactive Monitoring

Tracking new fraud patterns and tactics before they scale.



### Multi-Layer Defense

Combining automated detection with expert moderation review.



### Data-Driven Insights

Regular open reports to keep advertisers and partners informed.



### Ecosystem Transparency

Building trust through open communication about risks and enforcement.