



Bolster AI Fraudulent Ads Monitoring & Takedowns

Bolster AI identifies and removes fraudulent ads that impersonate your brand, hijack customer traffic, and redirect users into scam funnels. By stopping fraud at the point of acquisition, Bolster AI protects revenue, customers, and brand trust before the damage occurs.

How Attackers Steal Your Customers

Attackers Are Acquiring Your Customers

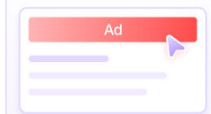
Modern fraud campaigns don't wait for victims. Attackers acquire customers using the same tactics legitimate businesses use — paid search, sponsored placements, and social promotion — to get the customer before the real company does. In practice, this shows up as:

-  Fraudulent ads impersonating your brand on your own branded search terms
-  Sponsored placements redirecting customers into fake storefronts and phishing pages
-  Keyword abuse capturing demand your marketing spend created
-  Scam funnels harvesting credentials and payment information from your customers
-  Campaigns reappearing under new advertiser accounts faster than teams can report them

1 Search



2 Fraudulent Ad



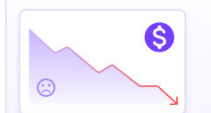
3 Fake Website



4 Credential Theft



5 Customer Impact



The Impact



Nearly 30% of 2025 scam losses started on social media ¹



\$3.5B reported lost to imposter scams in 2025 ²



1 in 3 ads may be a scam on social media in 2026 ³

How it Works

1 AI-Powered Detection

Continuously identifies fraudulent ads across paid search, sponsored, and social placements — before customers click or report the scam.

2 Evidence-Backed Removal

Takedowns are auto-filed through trust & safety channels with evidence — faster removals, fewer rejections, less manual work.

3 Funnel Suppression

Campaigns are investigated, not just single ads — attackers tracked across platforms and advertiser accounts so fraud stays down.

Citations

¹ FTC Data Spotlight: Reported losses to scams on social media eight times higher than in 2020, 2026

² FTC: People Reported Losing \$3.5 Billion to Imposter Scams in 2025, 2026

³ Gen Digital's The Scam Ad Machine: Part II (March 2026)

Key Benefits

-  **Revenue Protection**
Prevent attackers from intercepting demand that belongs to your business.
-  **Customer Protection**
Reduce exposure to scams, phishing, credential theft, and payment fraud.
-  **Brand Protection**
Ensure customers reach legitimate destinations associated with your brand.
-  **Faster Response**
Identify and remove fraudulent campaigns before they scale.
-  **Better Visibility**
Understand how customers are being directed into fraud campaigns.

What Makes Bolster AI Different

-  **Protects How Customers Find You**
Most tools focus on protecting websites, apps, and domains. Bolster AI protects the path customers take before they ever reach those destinations.
-  **Looks Beyond the Ad**
The ad is only the first step. Bolster AI investigates the redirect, destination, and supporting infrastructure.
-  **Built Around Real Fraud Campaigns**
One campaign may span fraudulent ads, fake websites, social impersonation, and phishing. Bolster AI uncovers those connections.
-  **Built for Security, Valued by Marketing**
Marketing feels the pain; security owns the fix. Bolster AI equips security to protect both.

Manual Process vs. Bolster AI

The difference becomes clear when compared to manual approaches:

Process	Manual Approach	 With Bolster AI
Ad Channel Coverage	Limited by manual searching, typically 1–2 channels	Monitors many ad channels
Time to Identify Fraudulent Ad	After customer complaints	Just minutes (with AI-powered detection)
Scope of Investigation	The ad alone	Ad, redirect, destination, and supporting infrastructure
False Positives Reviewed	Manual review required	Automated filtering; focus on real threats
Evidence Collection	Manual screenshots and documentation	Automated evidence packaging

Proven Results

-  **99.999%**
detection accuracy rate
-  **Up to 20X**
lower cost per takedown
-  **98.6% Manual Reduction**
Easing internal team workloads



Find it. Remove it. Stop the funnel.

See how Bolster AI Fraudulent Ads Monitoring & Takedowns can protect your customers, recover hijacked demand, and stop fraud before the first click.

[Request a Demo](#) 