Brand Misappropriation and Scam Ads: A Practical Response Guide

Your brand is being used in scam ads. What should you do next?

A practical guide for brand, agency and platform teams. · TrustRaise · October 2026

Criminals use trusted brand names, logos, products and spokespeople to make scam ads look legitimate. This guide helps brand teams respond when it happens and prepare for the conversations with agencies and platforms that follow. It assumes good intent on every side. Scam advertisers are well funded, technically capable and quick to change accounts, creative, domains and payment methods. Agencies and platforms are working on a difficult problem, and brands can help by supplying reliable evidence, clear records of what is authorized and consistent measurement.

This guide is vendor neutral and does not recommend specific detection providers. A companion one-page overview and a first-24-hours checklist are available separately.

Why this matters now

On October 22, 2026, Rhode Island Attorney General Peter Neronha filed what his office described as the first state lawsuit against Meta over scam advertising, following a similar case from Santa Clara County, California. The complaint alleges that Meta failed to curtail ads for fraudulent products, impersonation scams and fake investment offers, and that its targeting and optimization tools helped those ads reach people likely to respond. These remain allegations, and the Attorney General's release does not name any brands.

In September 2026 the FTC asked for public comment on whether to update its Impersonation Rule to address the role of platforms. The measures it asks about include vetting advertisers, monitoring ads, investigating suspected impersonation ads, removing confirmed ones and disciplining offending advertisers. This is an early request for comment, not a proposed rule.

Platforms are also investing. Meta reports removing more than 159 million scam ads in 2025, 92% of them before anyone reported them, and says verified advertisers will account for 90% of its ad revenue by the end of 2026, up from 70%. It says it uses AI to detect brand impersonation and lookalike domains. These are Meta's own figures. Opening a conversation by acknowledging this work sets a collaborative tone.

> Suggested opening: "With the Rhode Island case in the news, we wanted to check how we can protect our brand and customers together. We know this is a difficult problem and that scammers change accounts, creative, domains and payment methods quickly. We would like to understand what is already working, where the gaps are and what evidence we can provide to help."

1. How scam advertisers misuse brands

The method varies by industry. The common element is borrowed trust: the criminal uses something people recognize to lower their suspicion. Typical patterns include:

- Fake shops, promotions, giveaways and customer surveys
- Counterfeit or unsafe products sold under a recognized name
- Fake travel bookings, refunds and customer-support accounts
- Health products using a company's brand or a fabricated professional endorsement
- Investment schemes using executives, celebrities or public figures
- Fake recruitment ads and job offers
- Lookalike websites that collect payments, card details or account credentials
- Hijacked advertising accounts used to run unrelated scam campaigns
- AI-generated voices, faces and videos that appear to show a genuine endorsement

Reported examples include a fake Boots advert for a weight-loss drug and a deepfake video of David Attenborough endorsing a cryptocurrency scheme (Marketing Week, July 2026). Group-IB documented fake discount shops imitating brands such as Lego and Calvin Klein, promoted in Facebook and TikTok

deal-hunting groups, with some sites capturing card details as shoppers typed them (as reported by The Cool Down, October 2026).

The accounts behind the ads. Scam campaigns run from accounts the criminals create, accounts they buy and accounts they take over from legitimate advertisers. Mimecast says aged accounts with a clean history help ads pass checks that would block a new account, and cites one 2023 analysis with underground prices from about $15 to $340. A brand's own ad account is therefore both a possible target and a source of evidence when something goes wrong.

2. The cost to customers and to the brand

Cost to customers

- **Reported losses are large and rising.** People reported losing $2.1 billion to scams that started on social media in 2025, about eight times the $261 million reported in 2020. Investment scams accounted for $1.1 billion of that total (FTC).
- **Ads are a common starting point.** More than 40% of people who lost money to a social media scam said they ordered something they saw in an ad. Shopping scams were the most reported type, often through sites impersonating well-known brands with big discounts. Most people who reported them received nothing, and some received counterfeit goods (FTC).
- **Impersonation reaches beyond social media.** People reported losing $3.5 billion to imposter scams in 2025 across all contact methods, with nearly $1 billion tied to business impersonators (FTC).
- **Older adults carry a large share.** People aged 60 and over reported more than $3 billion in fraud losses in 2025 (FTC report to Congress, as summarized by PPC Land).
- **The harm extends beyond the payment.** Victims can also lose personal or payment information, access to online accounts, time spent contacting banks and platforms, and confidence in genuine advertising and in their own ability to spot a scam.

Cost to the brand

- **Trust falls even when the brand did nothing wrong.** 54% of consumers say their trust in a brand decreases after encountering a scam associated with it, and 58% report seeing a fake ad impersonating a well-known brand (Clutch).
- **Sales can be diverted.** A fake promotion, booking page, investment offer or shop can take a customer who intended to deal with the real company. The immediate cost may be one lost sale. The longer-term cost may include repeat purchases, referrals and willingness to respond to genuine advertising.
- **Genuine advertising can lose effectiveness.** Repeated exposure to fake offers can teach customers to distrust real ones, so they may avoid clicking, delay a purchase or contact the brand to check an offer.
- **Teams across the business carry the work.** Customer support, fraud investigation, legal and IP, agency and monitoring costs, repeated takedown requests, customer warnings, refunds or goodwill payments, and disruption to legitimate campaigns when an account or payment method is blocked.

No reliable public benchmark covers all of these costs, so each brand needs its own estimate. Measure around confirmed incidents rather than relying on a general industry figure. Section 7 lists what to track.

3. What to document when an incident appears

A complete record makes reports faster to review and gives the brand, agency and platform the same facts to work from. Capture the evidence before reporting, because an ad can disappear once it is flagged.

Area	What to capture
The ad	Ad ID, platform and placement, copy, full-page screenshots showing the URL and time, a screen recording of the click-through, and the ad library link
The advertiser	Account or page name and ID, profile link, any verification badge shown, and other ads from the same advertiser
The landing page	Final URL, every redirect, domain and hosting details if available, what the page asks visitors to enter, and how checkout behaves
Reach and timing	Date and time first seen, countries and languages, and impressions if the ad library shows them
Customer impact	Complaints, reported losses with personal details removed, and support contacts linked to the ad
Reporting	Who reported, the channel used, date and time, case number, platform response and time to removal
Handling	Originals stored in a shared folder, labeled with one incident ID, with a note of who captured each item

> Avoid entering real personal or payment details on a scam page while collecting evidence. If someone needs to test the click-through, use a device and account set aside for that purpose.

The companion first-24-hours checklist turns this list into an ordered set of steps.

4. Immediate account and payment checks

Two related risks sit behind many scam ads. Criminals may use stolen or fraudulent cards to fund their own campaigns, and they may take over a legitimate advertiser's account and spend through the payment method already attached to it. Mimecast recorded 6.4 million detections connected to ad account theft on Meta Business Manager and Google Ads over four years. That figure counts security detections across its customer base, not 6.4 million separate stolen accounts. Mimecast describes loss of account control, which can last weeks or months while appeals are processed, as the main harm to victims.

Account checks

- List everyone with admin or advertiser access to your ad accounts, pages and business managers, including agency and freelancer users, and remove anyone you do not recognize.
- Confirm two-factor authentication is on for every admin and that a backup administrator exists.
- Look for ads, campaigns, pages or linked domains that nobody on the team created.
- Set spending alerts and limits where the platform allows them.

- Agree in advance who can stop spend and how, if your team loses access to an account.

Payment checks

- Review card and invoice activity for charges you do not recognize.
- Remove payment methods that are no longer needed.
- If you see unauthorized charges, contact the card issuer quickly. Mimecast advises victims to remove linked cards and call the issuer.
- Keep a record of disputed charges alongside the incident record.

When an unauthorized card payment is disputed successfully, the payment to the platform may be reversed. Who bears the final cost depends on the transaction, its authentication and the card network rules. There is no reliable public figure for the share of scam ad spend paid with stolen payment methods, so treat that as a question for platforms rather than a statistic.

5. Questions for your agency

Agencies work closest to the ads every day. Frame these as a request to compare notes and open with appreciation for what they already do.

Current detection

- How do we find out today when our name, logo, products, executives or creative appear in a scam ad? Is it active monitoring, customer reports, social listening or a mix?
- Does the monitoring cover Meta, TikTok, search, display, marketplaces and the sites that ads send people to?
- Do we check advertiser accounts, landing pages and lookalike domains as well as the ad creative?

Technology and outside support

- Are you working with a technology partner to detect misuse of our brand? Which channels, countries and languages does it cover?
- Can it detect altered logos, copied creative, lookalike domains and AI-generated versions of recognized people?
- Does it connect directly to platform reporting systems, or does someone submit each report by hand?
- Where are the main gaps in current coverage?

Reporting and removal

- When something is found, who reports it, through which channel, and what evidence is saved first?
- How long does removal usually take, particularly when people are actively losing money?
- When the same advertiser returns under a new account, how is that identified and handled?
- Do you have direct platform contacts for confirmed impersonation cases, and how often are they used?

Account security

- How are our ad accounts protected against takeover, who has access today, and how often is access reviewed?
- How would we stop unauthorized spending if our team lost access to an account?

Ownership and measurement

- Can we receive a monthly view showing incidents, platforms, countries, estimated exposure, removal times and repeat offenders?
- Where does this work sit between media, social, customer service, legal and brand protection, and where do you see gaps?
- What information from us would help you detect and report cases faster, and what would you most like the platforms to change?

6. Questions for your platform partners

Check each platform's current advertising policy and brand reporting route before the meeting, and open with what it already offers. If time is short, ask the five questions marked with a star. They match the one-page overview.

Roadmap and prevention

★ What is planned over the next 6 to 12 months to detect ads that impersonate brands, including lookalike domains, copied creative and AI-generated voices, faces or videos?

- How do you verify the person or business paying for an ad, and when does an advertiser face extra identity, business or payment checks?
- How does advertiser verification prevent someone from claiming a relationship with a brand they do not represent?
- How do you inspect redirects and the final landing page when advertisers hide what visitors will see?

Brand information and reporting

★ Can we register our official accounts, domains, apps, logos, products and authorized agencies so matching happens before ads run, and what is the fastest route for confirmed misuse?

- What evidence leads to the quickest and most reliable decision, and what response time should we expect when customers are actively losing money?
- Can brands and agencies submit reports in bulk or through an API, and can the person reporting see the status and reason for the decision?

Advertiser-level enforcement

★ When one ad is confirmed as fraudulent, do you review the advertiser's other ads, accounts, domains and payment methods?

- How do you prevent a confirmed scammer from returning through a new account or advertising partner, and do you search for related versions in other countries and languages?
- How do you tell a compromised legitimate advertiser from the criminal controlling its account, and how quickly can the real business recover?

Payments

★ How do you detect stolen cards being used to buy ads, and could you share aggregate data on spend that is later disputed or reversed?

- What happens to an advertiser's other campaigns when a card payment is disputed as unauthorized?

- Could stronger card authentication or temporary limits for high-risk new advertisers help?

Partnerships and shared intelligence

★ Which partnerships with banks, card networks, brands, agencies, law enforcement and specialist detection companies are producing the best results, and where would brand and agency input help most?

- Can confirmed scam domains, advertisers and payment signals be shared across platforms, and could selected brands join a pilot?

Transparency and measurement

- Can you report separately on ads involving brand impersonation, including how many your systems found before a brand reported them?
- Can you report repeat-offender rates, average time to removal, and whether enforcement stops the advertiser from returning rather than only removing single ads?

> **Context to have on hand, not to lead with.** In a test between December 2025 and March 2026, BEUC and 13 national consumer groups reported 893 suspected fraudulent financial ads on Meta, TikTok and Google. BEUC says Meta rejected nearly 43% of the ads submitted, TikTok removed 21% and Google removed 60%. These were financial ads, not brand misuse, so the result is background for question 8 rather than a benchmark.

7. Measures the brand should track

A small set of consistent measures lets the brand, agency and platform see whether detection and removal are improving. Agree the definitions together before the first review.

Area	Measures
Scale	Number of confirmed incidents; estimated impressions before removal
Speed	Time from first appearance to detection; time from report to removal
Detection	Percentage found by monitoring or the platform before a customer reported it
Repeat activity	Percentage involving a repeat advertiser, domain or creative; percentage of cases where related ads stayed active after one was removed
Customer impact	Customer complaints and confirmed losses linked to the misuse; changes in conversion and complaints around major incidents
Account security	Account takeover and unauthorized spending incidents; recovery time for compromised accounts
Cost	Support, fraud, legal and communications hours; agency, monitoring and takedown costs; refunds or goodwill payments; time a legitimate account could not operate

This will not capture every reputational effect. It gives the business a figure it can defend and monitor, and a way to show agencies and platforms where progress is happening.

Appendix: Evidence

Figures below were checked against the linked pages in October 2026. Where a figure comes from a secondary report, the note says so.

Figure	Source	Note
$2.1 billion reported lost to social media scams in 2025, about 8 times the $261 million in 2020	FTC Data Spotlight, April 2026	Reported losses only
More than 40% of people who lost money to a social media scam ordered something they saw in an ad; 28% of all people who lost money to a scam said it began on social media	FTC Data Spotlight, EMARKETER	Facebook had the highest reported losses, then WhatsApp and Instagram
$3.5 billion reported lost to imposter scams in 2025, nearly $1 billion to business impersonators	FTC press release, June 15, 2026	All contact methods
People 60 and over reported more than $3 billion in fraud losses in 2025	PPC Land summary of FTC report to Congress	Secondary report
54% trust a brand less after a related scam; 58% saw a fake ad impersonating a well-known brand	Clutch release via Business Wire, March 2026	Sample size and fieldwork dates not confirmed
6.4 million detections of Meta Business Manager and Google Ads account theft over four years	Mimecast	Detections across its customers, not separate accounts
Rhode Island lawsuit filed October 22, 2026	Rhode Island Attorney General	Allegations; no brands named
FTC request for comment on platform role in impersonation scam ads	FTC press release, September 2026	Advance notice; comments due 60 days after Federal Register publication
About 10% of Meta's 2024 revenue (about $16 billion) linked to scam or restricted-goods ads; 15 billion higher-risk scam ads shown per day	Reuters reporting, via the Rhode Island release and The Next Web	Reported internal estimates; Meta called them rough and overly inclusive
159 million scam ads removed in 2025, 92% before being reported; verified advertisers to reach 90% of ad revenue by end of 2026	Meta newsroom, March 2026	Self-reported
893 suspected fraudulent financial ads; Meta rejected nearly 43%, TikTok removed 21%, Google removed 60%	BEUC	Financial ads, December 2025 to March 2026
Fake shops promoted on Facebook and TikTok capturing card details at checkout	The Cool Down on Group-IB research, October 11, 2026	Secondary report
Share of scam ad spend paid with stolen cards	No published figure found	Raise as a question

Working with TrustRaise

TrustRaise is a brand safety and trust and safety advisory led by Dave Byrne, who has worked at Google, TikTok, Spotify and IPG Mediabrands. If it would help to talk through an incident, review your response process or prepare for a conversation with your agency and platform partners, a free 30-minute call is available.

Dave Byrne, Founder, TrustRaise · dave@trust-raise.com · trustraise.com