AGENARYS · FREE FIX GUIDE

REVIEWS & REPUTATION · 3 POINTS · GUIDE 18 OF 27

Protect Your Reviews from Fakes and Attacks

What to do when the reviews aren't real — and the federal rule you need to know about.

TIME	COST	DIFFICULTY	AUDIT SIGNAL
1 hour	Free	Easy	review_integrity

WHAT WE MEASURED

We assessed your review profile for signs of manipulation, attack patterns, or policy problems.

WHY IT MATTERS

Two separate risks live here.

Someone attacking you — a competitor, a disgruntled ex-employee, or an extortion operation running a burst of fake one-stars followed by a demand for money.

You breaking a federal rule. The FTC's **Rule on the Use of Consumer Reviews and Testimonials (16 CFR Part 465)** took effect **October 21, 2024**. It carries civil penalties of **over $50,000 per violation** (the figure is adjusted for inflation annually). "Per violation" has been read to mean per fake review — so it compounds fast.

The part most owners miss: **"knowing" includes "should have known."** If you hire a review-generation vendor and never ask how they produce reviews, you are exposed to their conduct.

FIX IT YOURSELF

1 Know what the FTC rule actually prohibits

- **Fake reviews** — writing, buying, selling, or spreading reviews from people who don't exist or never used your service, including AI-generated reviews presented as real customers.
- **Paying for sentiment** — compensating anyone for a review "expressing a particular sentiment." This includes paying for **negative** reviews of a competitor.
- **Insider reviews without disclosure** — reviews from your officers, managers, employees, or agents must clearly and conspicuously disclose the relationship. The disclosure must be **unavoidable**; a consumer must not have to click a link to find it. This also covers asking your own employees, or their relatives, for reviews.
- **Company-controlled "independent" review sites** — running a "Top 10 Best [Industry] in [City]" site that quietly ranks you first.
- **Review suppression** — using unfounded legal threats, physical threats, or intimidation to remove a negative review. *(Sorting your own reviews by rating, helpfulness or date is explicitly fine.)*
- **Fake social media indicators** — bought followers, likes, or views.

Get a written representation from any reputation vendor that they comply with 16 CFR Part 465 and with the platform policies of every site they touch.

2 Spot an attack

Signals, most reliable first:

- A cluster of one-star ratings within hours or days, often with no text
- Reviewer profiles with no photo, one review ever, or a burst of reviews across unrelated businesses in distant cities
- Content describing a service you don't offer or a location you don't have
- Reviews naming a competitor favourably
- Any rating drop that coincides with an inbound message demanding money

Real bad reviews are specific, dated, and matchable to an actual transaction. Fakes are generic and clustered.

3 Report the review the right way

Use the **Reviews Management Tool** — it gives you a trackable case, unlike the in-profile flag:

support.google.com/business/workflow/9945796

1. Confirm the email associated with the profile.
2. Select your business → **Report a new review for removal**.
3. Select the review → **Report**.
4. Choose the violation reason → **Submit**.

Evaluation typically takes several days. If denied, **you get one appeal** — return to the same tool and choose "Check the status of a review I reported previously." Make it count: write the appeal around the **specific policy clause** violated, quote it, and attach evidence that the reviewer was never a customer.

Common mistake: the *Business Redressal Complaint Form* is widely and wrongly recommended for fake reviews. It's for fraudulent **listing data** — a competitor faking their address or hijacking your phone number. Not reviews.

4 If someone demands money — do not pay

Google has a dedicated channel for review extortion. Their description of the pattern: *"a sudden increase in 1-star and 2-star reviews… followed by someone demanding money, goods, or services in exchange for removing the negative reviews."*

Report at: support.google.com/business/contact/merchant_extortion

Gather first: screenshots of every demand, direct links to each suspicious review, any names/emails/phone numbers/social profiles of the perpetrator, and the dates the reviews and demands started.

Google's explicit instruction: *"Do not engage with or pay the malicious individuals. This can encourage further attempts and doesn't guarantee the removal of reviews."*

Also report to the **FBI IC3** at **ic3.gov** — this is extortion, a crime — to the **FTC** at **reportfraud.ftc.gov**, and to your state Attorney General.

5 Set expectations on what gets removed

Removal succeeds when you can point to a **policy clause**, not when a review is unfair.

Gets removed: not a genuine experience · conflict of interest · off-topic · profanity or harassment · personal information · promotional content · impersonation.

Does not get removed: harsh but real · factually mistaken · one star with no text · from a customer you fired.

Most legitimate negative reviews will stay. Your response is the remedy — see *Respond to Every Review*.

6 Respond calmly to fakes while the case is pending

Prospects reading your profile need to see a business behaving normally. Keep it short and non-accusatory:

> *"We have no record of this visit and have reported this review for investigation."*

Don't accuse anyone. Don't name anyone. Don't argue.

CHECK YOUR WORK

- ☐ You've reviewed your profile for attack patterns.
- ☐ Any suspicious reviews are reported through the Reviews Management Tool.
- ☐ You have written compliance assurance from any reputation vendor.
- ☐ No employee, family, or insider reviews sit on your profile undisclosed.
- ☐ You know the extortion reporting path and would not pay.

COMMON MISTAKES

- **Buying reviews.** Over $50,000 per violation, and 'should have known' counts.
- **Employee reviews without disclosure.** A federal rule violation, not just a Google one.
- **Legal threats to reviewers.** Prohibited by the FTC rule itself.
- **Paying an extortionist.** It marks you as a payer and invites more.

This fix is free. You can earn and keep any Agenarys Seal tier — including Platinum — without paying Agenarys anything beyond the audit itself. If you would rather have help doing it, we sell that. We never sell passage.

SOURCES & FURTHER READING

FTC Rule on the Use of Consumer Reviews and Testimonials, 16 CFR Part 465 (eff. Oct 21, 2024)
FTC Q&A: ftc.gov/business-guidance/resources/consumer-reviews-testimonials-rule-questions-answers
Civil penalty amount, 16 CFR § 1.98 — adjusted annually; confirm the current figure
Google Reviews Management Tool: support.google.com/business/workflow/9945796
Google review extortion reporting: support.google.com/business/answer/16404809

Agenarys · Operational Intelligence Audit · Standard v2026.1 Issued July 2026 · agenarys.com/guides/review-integrity

Content reviewed July 28, 2026 | Next review: January 2027 (annually)