Know the Tactics. Keep the Choice.

A practical consumer guide to recognizing manipulative pricing, misleading offers, and unfair buying experiences
Scott's Red Stapler Award · Consumer Resources
Updated November 2026 · U.S. edition

You should know what you're agreeing to.

You can be a careful shopper and still get caught by a misleading offer. A price changes at checkout. A free trial quietly becomes a subscription. A checkout screen makes declining an add-on unusually difficult. A product looks familiar, but the package contains less.

Businesses know a great deal about how people make decisions. Some use that knowledge to make buying easier. Others use it to make us spend more, overlook important information, or give up when trying to cancel.

This guide is about getting your ability to choose back. Each tactic includes a warning sign, something you can do about it, and a free source where you can check the evidence yourself.

One important distinction: An unpleasant practice is not necessarily an illegal one. Dynamic pricing, discounts, subscriptions, and smaller packages can all be legitimate. The questions are whether you received truthful information, understood the terms, and had a meaningful choice. Laws vary by product, state, and circumstances.

The 60-second check before you pay

1. **Final price:** What is the total, including mandatory fees, shipping, and taxes?
2. **Real quantity:** How much am I getting per ounce, item, hour, or month?
3. **Real deadline:** Is this offer genuinely time-limited, or is the website pressuring me?
4. **Future charges:** Will this renew or charge me again? When, and for how much?
5. **Extra items:** Did anything get added to my cart or agreement without an intentional choice?
6. **Independent proof:** Are reviews, rankings, and endorsements independent or paid?
7. **Exit route:** How do I return it, cancel it, or dispute the charge if something goes wrong?

If the seller makes those answers hard to find, slow down. You do not owe a business an immediate decision.

14 tactics worth recognizing

1. The price that grows at checkout

Also called: *Drip pricing* or *hidden mandatory fees*.

What it looks like: A ticket, hotel stay, or service is advertised at one price. You invest time choosing it, then required fees appear near payment. By then, leaving feels like wasting the effort you already spent.

Protect yourself: Compare the **all-in total**, not the headline price. Take a screenshot of the original offer and the final checkout amount. If mandatory charges appear late, ask for an itemized explanation or shop elsewhere.

What the law actually says: The FTC's federal fee rule, effective May 2025, specifically covers **live-event tickets and short-term lodging**, not every retail purchase. It requires upfront disclosure of total prices including most mandatory fees, with limited exclusions. Other misleading pricing may still violate broader consumer-protection laws. [Sources 1, 2]

2. Dynamic Pricing: A price chosen for you

Also called: *Personalized pricing*, *surveillance pricing*, or *price discrimination*.

What it looks like: An offer or discount may depend on your location, browsing behavior, shopping history, or information inferred about you. The FTC reported in 2025 that pricing intermediaries can use detailed consumer data to tailor prices and promotions. Its study did **not** prove that every retailer uses such methods or that every individual shopper pays more. [Source 3]

Protect yourself: Compare identical items across multiple sellers. Check the full price while signed in and, where practical, without signing in. Review app location and advertising permissions. Those checks may reveal differences, but private browsing is **not** a guaranteed way to obtain a lower price.

The distinction: Prices can legitimately vary by time, inventory, location, membership, or an advertised discount. The concern is hidden exploitation, misleading explanations, or unequal treatment that violates applicable law, not the mere existence of two prices.

3. The sale that may never have been a sale

Also called: *False reference pricing* or *price anchoring*.

What it looks like: A product displays "WAS $199, NOW $89." The larger number creates the impression of an extraordinary bargain, even if the item was rarely or never genuinely offered at that higher price.

Protect yourself: Search the exact model number and compare its current price at other retailers. For expensive purchases, use a price-history tracker when available. Judge the purchase against what it is worth **today**, not the crossed-out number.

The distinction: Genuine sales are normal. The FTC's Guides Against Deceptive Pricing distinguish bona fide former prices from invented or inflated comparison prices. [Source 4]

4. The countdown that tries to make you stop thinking

Also called: *False scarcity* or *manufactured urgency*.

What it looks like: "Only 2 left!" "Offer expires in 04:59!" or "12 people are viewing this." These messages can be legitimate, but they can also be designed to create pressure without a factual basis.

Protect yourself: Decide whether the purchase makes sense **without** the deadline. For a nonessential purchase, leave the page and return later to check whether the same countdown or deal reappears. A reset is a warning sign, although it is not conclusive proof of deception.

Why it matters: The FTC identifies misleading countdown timers as an example of deceptive interface design, often called a *dark pattern*. [Source 1]

5. The free trial that becomes a bill

Also called: *Negative-option billing* or a *subscription trap*.

What it looks like: You enter a card for a "free" trial. A recurring charge starts unless you cancel, or the paid renewal price is much higher than the introductory amount.

Protect yourself: Before enrolling, find the **first billing date**, **renewal amount**, **billing frequency**, and **cancellation method**. Save a screenshot. Put a reminder on your calendar a few days before the deadline. Keep written confirmation when you cancel, and review subsequent statements.

The distinction: Automatic renewals can be useful when disclosed and agreed to. The danger is missing or confusing material terms, enrollment without informed consent, or blocked cancellation. Some cancellation rights differ by state and service; do not assume one universal federal cancellation rule applies to every subscription. [Source 5]

6. The cancellation maze

Also called: *Obstruction* or *sludge*.

What it looks like: Signing up took two clicks. Canceling requires hunting through settings, calling during limited hours, sitting through repeated retention offers, or facing broken links.

Protect yourself: Ask for the cancellation procedure in writing. Screenshot the steps and any errors. Send a dated written cancellation request through an official support channel. Keep a record of attempts and check for further charges. If unauthorized billing continues, contact your payment provider promptly. [Sources 1, 5]

Keep this sentence: "I am canceling authorization for future recurring charges. Please confirm the effective date in writing."

7. The choice that was already made for you

Also called: *Preselected add-ons*, *sneak-into-basket*, or *misleading choice architecture*.

What it looks like: Insurance, priority service, donations, or an extended warranty is already selected. A big, bright button accepts data sharing, while the refusal option is faint or confusing.

Protect yourself: Review every line of the cart before clicking Pay. Uncheck anything you didn't deliberately select. On privacy screens, inspect both the prominent and less-prominent options. Keep the order confirmation to verify what was actually purchased.

The distinction: An optional add-on is not inherently problematic. The issue is whether the design leads you to pay for something or share data without a clear, intentional choice. [Source 1]

8. The privacy decision that isn't really a decision

Also called: *Privacy dark patterns*.

What it looks like: A screen makes "Accept all" obvious while "Reject" is buried. An app requests location access that may be unnecessary for the service you want.

Protect yourself: Check your phone's permission settings and the website or app's privacy controls. Give access only when you see a reason for it. Review permissions periodically; a useful app may still request more data than you wish to share.

The distinction: Data collection is not automatically proof of unfair pricing. Less unnecessary data sharing can reduce exposure, but it cannot guarantee a particular price or prevent every form of tracking. [Sources 1, 8]

9. The five-star wall

Also called: *Fake reviews*, *review suppression*, or *manufactured social proof*.

What it looks like: A business appears universally loved. The reviews repeat similar phrases, arrive in bursts, or seem disconnected from the actual product. Sometimes a company's own review site appears independent.

Protect yourself: Compare reviews across **independent websites**. Read detailed middle-rated reviews, recent critical reviews, and the seller's responses. Check whether reviewers have broader histories. Don't assume you can reliably spot all fake reviews by writing style alone.

What the law says: The FTC's reviews rule targets specified practices including certain fake reviews, paid reviews conditioned on sentiment, and some review suppression. [Sources 6, 7]

10. The recommendation that's actually an advertisement

Also called: *Undisclosed sponsorship*, *affiliate promotion*, or *native advertising*.

What it looks like: A creator, article, or comparison site recommends a product without clearly showing that someone benefits financially from the recommendation.

Protect yourself: Look for advertising, sponsorship, affiliate, and gifted-product disclosures. If a site claims to rank "the best" providers, check how it makes money and whether sellers pay for placement. Seek an additional independent source before large purchases.

The distinction: Paid recommendations are not automatically dishonest. Hidden material relationships can prevent consumers from judging credibility fairly; the FTC expects relevant relationships to be disclosed clearly. [Sources 1, 9]

11. The familiar package with less inside

Also called: *Shrinkflation*.

What it looks like: A package looks almost unchanged, but the net weight, number of sheets, serving count, or number of items is lower. The price may stay the same.

Protect yourself: Compare **unit prices**: price per ounce, pound, sheet, or item. Check the stated net quantity rather than the box's appearance. If the shelf label lacks a usable unit price, calculate it yourself: **total price ÷ total units**.

The distinction: Selling a smaller package is not itself illegal when quantities are accurately disclosed. Misleading packaging or quantity claims raise separate concerns. The FTC recommends checking net contents and unit prices. [Source 10]

12. The payment that looks smaller than the purchase

Also called: *Payment framing* or *buy now, pay later (BNPL)*.

What it looks like: "Only $25 today" appears more prominently than "$100 total." Installments can make spending feel smaller even when the full obligation remains.

Protect yourself: Write down the **entire amount owed**, every due date, and any late or other fees. Make sure several simultaneous installment plans don't exceed what you can realistically pay. A no-interest offer can still carry costs if payments are missed.

The distinction: Installment plans may be useful. The CFPB explains that many BNPL products charge late fees and that repayment problems can have additional consequences. [Source 11]

13. The low introductory rate with the expensive second act

Also called: *Teaser pricing* or *introductory-price framing*.

What it looks like: Internet, phone, software, or another recurring service looks inexpensive for a few months and then jumps to its regular rate. Important charges or contract conditions may be easy to miss.

Protect yourself: Ask: "What will my total monthly bill be **after** the promotion ends?" Write down the regular price, promotion end date, equipment fees, early termination terms, and any annual increases. Compare the cost over 12 months, not just month one.

The distinction: Temporary promotional rates can be legitimate. The risk is an unclear future price or terms that don't match the sales pitch. Keep a copy of the offer and your agreement. [Sources 5, 8]

14. The urgent repair or service upsell

Also called: *Pressure selling* or, in deceptive cases, *bait-and-switch*.

What it looks like: You call about one repair, but you're told you must immediately approve a far more expensive service. The provider resists putting the scope, necessity, or price in writing.

Protect yourself: When it is safe to do so, get an itemized written estimate with labor, materials, and alternatives. Ask what is urgent, what can wait, and what evidence supports the recommendation. For major projects, verify licensing where required and obtain more than one estimate. Don't sign an incomplete contract.

The distinction: A legitimate inspection can reveal a serious new problem. An expensive recommendation alone is not proof of deception. The FTC recommends written estimates, credential checks, and caution around high-pressure home improvement offers. [Source 12]

If you think you've been taken advantage of

1. Preserve the evidence. Save the advertisement, screenshots, product page, checkout total, contract, cancellation policy, emails, receipts, and dates of conversations. The order in which prices and terms appeared can matter.

2. Ask for a specific correction. Explain the difference between what was promised and what occurred. Request a refund, correction, cancellation, or itemized explanation. Ask for a response in writing.

3. Escalate quickly if money is at risk. For a credit-card billing error, the CFPB advises contacting the issuer immediately and sending a written billing-error notice to the appropriate address **within 60 calendar days after the charge first appeared on the statement** to protect federal billing-error rights. Other claims, debit-card transactions, and other payment methods can have different processes and deadlines. Don't wait for a merchant's internal complaint process to run out the clock. [Source 13]

4. Report conduct to the right place. Use the FTC's ReportFraud.ftc.gov for suspected scams, deception, or other bad business practices. For problems with a financial product or service, consider the CFPB complaint portal. Your state attorney general or state consumer-protection office may also be able to assist. Filing a report does not guarantee an individual refund. [Sources 14, 15]

A message you can send to a company

I purchased [product or service] on [date] after seeing an advertised price or term of [what was represented]. The final charge or actual term was [what happened]. I have attached the relevant screenshot, receipt, or confirmation. Please explain the difference and confirm [the specific refund, correction, or cancellation you want] in writing by [reasonable date].

Stay factual. Save copies. You don't need to accuse a company of fraud to ask it to account for what it promised.

The principle behind the guide

A business may understand pricing psychology, customer behavior, and purchasing data better than you do. That does not make every sale unfair. It does mean the information and power in a transaction are often unequal.

Being willing to pay something is not the same as being given a fair opportunity to understand it.

A reasonable marketplace gives people accurate information, meaningful choices, and a way to hold sellers to their promises. You shouldn't need to become an expert in behavioral economics to buy groceries, book a hotel, or cancel a subscription.

Use this guide before a big purchase. Share it with someone who needs it. The more clearly customers understand the tactics, the less effective the misleading ones become.

Sources and further reading

All sources below are freely accessible and were checked when this guide was prepared. The short annotations explain what each source supports. Government guidance describes general rules; legal rights depend on the facts and jurisdiction.

1. FTC: Bringing Dark Patterns to Light (overview). Explains misleading countdowns, obstructive cancellation, preselected choices, hidden fees, and privacy-related interface tricks.

2. FTC: What the Rule on Unfair or Deceptive Fees Means for You. Consumer-friendly explanation of upfront total-price requirements for live-event tickets and short-term lodging; the rule does not cover every retail sector.

3. FTC: Surveillance Pricing Study: Initial Findings (2025). Describes information that pricing intermediaries can use to tailor prices and offers; not proof that all retailers use personalized pricing.

4. FTC: Guides Against Deceptive Pricing (16 CFR Part 233). Federal guidance on genuine versus fictitious former prices and misleading bargain claims.

5. FTC: Getting In and Out of Free Trials and Auto-Renewals. Practical checklist for recognizing recurring billing terms and documenting cancellation.

6. FTC: How to Evaluate Online Reviews. Consumer advice on cross-checking reviews and spotting suspicious review patterns without assuming every suspicious review is fake.

7. FTC: Final Rule Banning Fake Reviews and Testimonials. Describes practices covered by the FTC's consumer reviews and testimonials rule.

8. FTC: Online Shopping. How to compare total costs, investigate sellers, check return terms, save records, and review shopping-app data collection.

9. FTC: Disclosures 101 for Social Media Influencers. Explains why material financial or other relationships should be made clear when recommending products.

10. FTC: The Case of the Shrinking Packaging. Explains how net-content labels and unit prices help shoppers spot shrinkflation.

11. CFPB: Do Buy Now, Pay Later Loans Have Fees?. Covers late fees and other consequences of missed installment payments.

12. FTC: How to Avoid a Home Improvement Scam. Guidance on written estimates, license checks, contracts, payment timing, and pressure selling.

13. CFPB: How Do I Dispute a Charge on My Credit Card Bill?. Explains the written-notice deadline and dispute procedure for qualifying credit-card billing errors.

14. FTC: ReportFraud.ftc.gov. Official place to report suspected scams, deceptive offers, and bad business practices.

15. CFPB: Submit a Complaint. Official portal for complaints about consumer financial products and services.

Editorial note: This guide is independent consumer education, not individualized legal advice. It is not a claim that every business using one of these approaches has broken the law. Scott's Red Stapler Award is not affiliated with the cited organizations.