Ohio Attorney General's

# Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

**August 2025**

## Know your rights: FTC's rule on unfair or deceptive fees

The Federal Trade Commission's new rule on unfair or deceptive fees took effect in May. The rule, which aims to stop bait-and-switch pricing, requires businesses to include all mandatory fees in the advertised price for certain purchases, particularly live-event tickets and short-term lodging.

This means businesses can no longer advertise a base price and later tack on charges such as processing a fee on a live-event ticket, a per-day fee on a hotel room, or a cleaning fee on a vacation rental.

The rule applies to any business — whether online, in-store, or through an app — that offers, displays, or advertises:

- Live-event tickets for concerts, sports, theater, or other in-person performances.

- Short-term lodging, including hotels, motels, inns, and vacation rentals (e.g., Airbnb, VRBO), as well as discounted extended stays.

**Not covered** under the rule:

- Long-term housing or landlord-tenant leases
- Lease extensions from rental providers
- Corporate housing offered under long-term lease terms

**Note:** A "short-term" stay is not defined by any set duration — it depends on the nature of the accommodation.

**Fees that *don't* have to be included upfront:** There are a few fees or charges that a business can disclose later in the transaction, as long as it discloses them before asking for payment. The total price displayed upfront need not include:

- Taxes or other government charges.
- Shipping charges.
- Charges for optional goods or services that people may buy as part of the same transaction.

*Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.*

---

## Scammers invading Ohioans' smartphones via text messages

Scammers are working overtime to send out phony package-delivery notices falsely claiming to be from UPS, FedEx, or the U.S. Postal Service.

Although the real package couriers send out legitimate notices to customers, the scammers operate to confuse and mislead consumers into clicking on bogus links that request money and/or personal information. The scammers often falsely suggest that there is a "problem" with an upcoming delivery that could divert or delay the package delivery.

To avoid becoming a victim of such scams, the Federal Trade Commission advises you to:

- Always verify information about your expected delivery using the retail websites from which you bought the product or service — it's typically where the legitimate shipping and tracking information can be found.
- NOT click on any links in text messages that might be a hoax; they could infect your device with malicious software.
- Determine whether your mobile device has filters to block text messages from unknown senders or other options to alter the delivery of junk text messages. For example, some devices allow you to send unknown texts to a special "Spam & blocked" folder.
- Report junk and scam text messages. If your device has an option available to report it, do so. If not, forward the suspicious text messages to 7726 (SPAM). For more information about this reporting function and how to forward a text message, click here.

Additionally, many Ohioans have reported receiving fraudulent text messages demanding that they immediately pay an unpaid toll fee or parking ticket. Such messages often claim to be from the Ohio Turnpike, E-Z Pass or another state's toll authority. The Ohio Attorney General's Office reminds readers:

- Do NOT click links or provide payment information.
- Verify directly by contacting the toll authority or parking service through official channels.
- Report scams to the Ohio Attorney General's Office at 800-282-0515.
- Stay alert and stay informed.

Also, check out the Attorney General's Phone Scams Checklist as well as information and tips from the FTC "to help you weed out spam text messages, phishing emails, and unwanted calls."

*Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.*

---

## Motor vehicle-related scams pose pitfall

Do you know what yields the most consumer complaints with the Ohio Attorney General's Office?

Motor vehicles.

Complaints include those from consumers who have lost money attempting to purchase vehicles or farm equipment from fake websites.

Scammers' prices often are significantly lower than expected, and they may have a legitimate-looking website with many pictures. Oftentimes, the scammers "clone" the inventory of a legitimate dealer or use the name and/or address of a real business that doesn't have a website. In such cases, searching for the business by name or address may yield results indicating that the business is well-established, providing false security to the unassuming buyer.

To avoid losing money through a fictitious posting or website, look for these red flags:

- If the price is too good to be true, it probably is.
- Check the website's registration information at www.whois.com/whois. This site shows when the website address was registered, which often is within the past few months if the site is fraudulent.
- Scammers often offer "free delivery."
- Money transfer services (such as Western Union or MoneyGram), cryptocurrency and gift cards are often the preferred methods of payment of scammers.
- Some scammers offer to use a fake "escrow service" to make the transaction seem safe. Watch out for scams that purport to be affiliated with legitimate companies, such as eBay or PayPal; sometimes scammers even use the logos of the real companies.
- Download one or more of the photos from the website and conduct an image search using Google or a similar search engine. Scammers often steal photos from legitimate websites or use stock photos, so check whether the exact images can be found online on other webpages.
- Be wary of a seller who is unwilling to meet in person.

- Don’t buy motor vehicles or farm equipment without first seeing it in person. Steer clear of making deposits or down payments before seeing the vehicle firsthand.
- Don’t be rushed. Scammers try to create a false sense of pressure by claiming there are other interested buyers and that you need to act right away to secure the purchase.

The Attorney General’s Office has fielded some complaints recently about the bill of sale for the vehicle not accurately reflecting the transaction between the buyer and the dealership. The bill of sale — essentially a receipt — should properly list the vehicle being purchased (including the VIN), the total vehicle cost, the odometer reading at the time of sale, both the dealership’s and consumer’s mailing addresses, and other details about the transaction. Consumers should carefully review the bill of sale for accuracy before finalizing the transaction with the dealer.

Finally, every financed motor-vehicle sale must include a disclosure box with information under the federal Truth in Lending Act. The box explains to the consumer the true cost of financing the vehicle, including the interest rate, down payment amount, purchase price, cost of interest payments, and overall cost of the vehicle (with interest and principal payments). Consumers should carefully review the Truth in Lending Act information before completing the sale.

Consumers in the market for a used motor vehicle should review the Ohio Attorney General’s Used Car Buyer Checklist for tips on how to find the right dealership and the right vehicle for you.

*Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General’s Office at www.OhioProtects.org or 800-282-0515.*

---

## Parental controls are key to keeping children safer online

Computers, tablets and smartphones are  being used constantly by young people at home and at school. A discussion about the family rules regarding devices and parental controls can ensure your children’s online safety.

Parental controls allow a parent to limit and monitor what a child sees and does online. They can be set at the device level, operating-system level, or app level.

*At the device level:*

A device is the actual piece of equipment your child is using. Most commonly, this is a phone, tablet, computer, or gaming system. Device controls apply to the entire device, not to a specific user. For example, for a shared computer, the controls are set for the entire computer, even though individual users have different controls. Parental controls, such as screen-time limits for  a single day, can be placed on a device.

*At the operating-system level:*

An operating system allows your device to run. On mobile devices and tablets, the two most common operating systems are iOS (Apple) and Android (Google). You can generally set operating-system controls on a per-user basis. Through the operating system, you may be able to restrict apps that can be downloaded, set screen-time limits across devices, and set age controls. You may also be able to link family members to control their devices through their devices.

*At the app level:*

An app is an individual program, many of which have customizable user experiences. Most apps have different privacy controls (for adults and kids) and may offer distinct experiences for users of different ages. They also may have an age rating based on content factors such as violence and language. Parents may be able to limit in-app purchases via the app directly.

Privacy settings, which control what others can see about a user, are especially important for children. Many apps default to public profiles or public sharing. Parents should consider changing these settings to private. For example, you may need to adjust an app's "location settings" to prohibit others from knowing your child's whereabouts.

Talk to your children about the importance of not revealing personal information in posts and user profiles, including photos that contain identifiable information.

Although specific settings and functions vary based on the parental controls you use, the Federal Trade Commission suggests the following:

- Manage how much time your kid spends online.
- Restrict the type of content your kids can access.
- Get information about your kids' websites and app activities.
- Limit who your children can communicate with.
- Restrict purchases.

To work best, parental controls need to be set up on all the devices your kid uses. It can seem overwhelming, but one of the suggested tools might give you the options you're looking for. You can always add other tools or settings later.

For more information, the Ohio Attorney General's Office publishes Social Media Pointers for Parents. The FTC, too, offers free online publications.

For more general cybersecurity tips, visit www.OhioAttorneyGeneral.gov and review the Cybersecurity Help, Information and Protection Program (CHIPP) booklet.

*Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.*