Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

August 2024

Best practices for avoiding ticket scams

Summer and fall are popular seasons for concerts and sporting events, including high-profile attractions that sell out quickly. Scammers know that in the rush to secure tickets, people may let their guard down. Here are some tips to avoid falling victim to ticket scams:

- **Be skeptical of offers that seem too good to be true.** Sellers on online marketplaces might offer tickets at face value (or below) for events that are sold out or in high demand, but these offers could be scams. Some may provide dubious explanations for why they need to sell tickets quickly – falsely claiming, for example, that they have a medical emergency or an overseas military assignment.

- **Review the venue's seating chart.** One way to check whether the tickets are valid is to familiarize yourself with the venue's seating chart. If the seller is offering a seat in a row number not listed on the chart, it's likely a scam.

- **Ask for the original ticket confirmation.** When buying from an individual who purchased the tickets through an online ticket seller, ask the person to send you the confirmation email sent by the original seller. Don't send any money until you verify that the tickets are real.

- **Be cautious when dealing with third-party sellers.** To protect yourself, deal with reputable businesses instead of third-party individuals unaffiliated with an event. Sophisticated but illegitimate websites can easily impersonate logos. Before providing any payment or personal information, research a seller's reputation, especially that of an individual seller. Search the seller's name, username, email address, phone number and other details for information. Even if you find no negative information, don't assume that the seller is trustworthy. Some con artists change their names regularly.

- **Think twice if the seller contacts you first.** If someone you do not know contacts you out of the blue offering tickets to a sold-out sporting event or concert, it might be a scam.

- **Be cautious when buying on social media.** Sellers might market to their friends on social media but be sure you're actually buying from a known friend. Accounts can get hacked, and scammers sometimes pose as trusted friends to sell their tickets; once you send the money, the tickets don't arrive. Contact your friend in another way – call or text – to see if the offer is legitimate before sending money.

- **Be wary of sellers who change the requested form of payment.** Con artists often request payment methods that are difficult to trace or recover, such as wire transfers, cash or gift cards. If you're using a mobile wallet or peer-to-peer payment service such as Venmo or Zelle, be sure that you understand the protections the service provides (and doesn't provide) before making a transaction. If buying from a ticket resale site, understand the protections that it offers, too.

- **Consider paying with a credit card.** If a problem arises, you generally have greater protections and the ability to dispute charges with a credit card. The same isn't true for some other payment methods.

Consumers who believe they have been defrauded should immediately report the details and contact the company they used to make the payment. Ohioans can report scams to the Ohio Attorney General's Office at www.OhioProtects.org or by calling 800-282-0515.

Debt collection: Know your rights

Some Ohioans struggling to make ends meet may find themselves receiving phone calls or letters from third-party debt collectors. Once your missed payment is turned over to a third-party collector, you have rights under the federal Fair Debt Collection Practices Act.

It can be difficult to tell a phony debt collector from a legitimate debt collector, but learning your rights can help spot a scam.

In general, the Fair Debt Collection Practices Act governs how collectors can contact you and the methods they can use. It's important to note that the act applies only to third-party collectors, meaning

if a company is collecting on its own behalf, it's not subject to the restrictions. Here are some of your consumer rights when dealing with a third-party debt collector:

- A debt collector must send you a notice (electronic or postal mail) within five days after contacting you by phone, including how much you owe, who you owe it to, any related account number, and how long you have to dispute the debt. This is known as a validation notice. A phony debt collector probably will not take this step.

- You have 30 days from the date of first contact to send a letter disputing the debt and specifically requesting verification of the debt. The debt collector must not contact you again unless the collector sends proof that you owe the money.

- Whether or not you owe the debt, you can tell debt collectors in writing not to contact you again. That does not eliminate the debt but stops further communication from the collector.

Third-party debt collectors may not:

- Harass you or use obscene language.

- Contact you before 8 a.m. or after 9 p.m.

- Contact you without identifying themselves.

- Use false names or statements, such as falsely implying that they are attorneys, government representatives or credit bureau representatives.

- Threaten you or your family with harm.

- Disclose your debt to others. If debt collectors know you have an attorney, they can contact the attorney and no one else, with very limited exceptions such as a spouse. Otherwise, they can contact others, such as neighbors or relatives, but only to find out how to reach you. Generally, they cannot contact third parties for any other reason unless you have given them prior consent to do so.

- Contact you at work if you or your employer disapproves.

- Falsely represent that you have committed a crime.

- Misrepresent the amount you owe.

Debt does not expire or disappear until it's paid. If a debt is valid, you still owe it until you pay it off, no matter how much time passes. However, the law limits the amount of time during which a debt collector may take legal action to collect a debt. Statutes of limitation vary depending on the type of debt.

Even if your debt is several years old and the statute of limitations has expired, it may still be reported to the credit-reporting agencies and can negatively affect your credit score. Accurate negative

information can stay on your credit report for up to seven years; bankruptcies stay on your credit report for 10 years.

Always read all correspondence you get from a court or debt collector's attorney. These papers contain important information about court dates and other obligations. If you get served with court papers, do not ignore them.

For more information about getting sued by a debt collector, visit Ohio Legal Help at www.ohiolegalhelp.org. To find a civil legal aid provider, call (866) LAW-OHIO (866-529-6446).

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.

New AG publication offers social media tips for parents

Understanding and managing your children's use of social media can feel overwhelming. Deciding how and when to allow them to use these platforms is a personal choice. The Ohio Attorney General's Office has compiled information to help families make informed decisions.

A social media platform is any internet-based platform that allows users to interact, create, share or exchange information with others. Common social media platforms for children include TikTok, YouTube, Snapchat, Instagram, Facebook, BeReal and even certain gaming communities, such as Roblox and Minecraft.

According to the new AG's publication, Social Media Pointers for Parents, there are five fundamental action steps parents can take:

Start and maintain an open dialogue. Have open and honest discussions with your children about their use of social media, including which platforms they currently have or want to use. Discuss your expectations as a parent and explain the controls and limits you will be setting. Encourage your children to tell you immediately if something happens that makes them feel uncomfortable or puts them in danger.

Learn about the social media platforms your children use. The more you know about each social media platform, the better you'll understand how the platform operates and what potential dangers, risks and challenges exist.

Follow age requirements and guidelines. Many social media platforms have age limits for joining; some may offer a version for kids that has stricter privacy and messaging settings.

Help set and monitor privacy settings. 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; consider changing these settings to private. Talk to your children about the importance of not revealing personal information in posts and user profiles, including photos that may contain identifiable information.

Understand how technology can help you. Devices and user accounts generally have various permission levels. For example, you might be able to set controls so your child cannot download an app without your permission. Private content filters also exist that give parents the ability to control content or apps, set privacy rules, limit screen time and more.

It's essential that parents and children understand the social media platforms they're using. Families should talk openly about how children should use the platforms and how to report inappropriate behavior. Also, consider setting rules in your house about where your children are allowed to have their devices and how many hours per day (and which hours) your children can be on their devices.

For additional resources, the Federal Trade Commission (FTC) offers free online publications to help keep kids safe online.

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

Protect yourself from phone, text and email scams

Impostor scams occur when a fraudster pretends to represent government institutions, private companies and charitable organizations. Be cautious of anyone seeking to confirm your personal information via phone, text or email.

Government impostor: A scammer might pose as a representative from a government agency such as the IRS, the Social Security Administration or a local court. They might demand payment for back taxes or an old court fee and threaten to arrest you if payment is not made immediately. The scammer might also request personal information, such as your Social Security number. Do not provide any information – hang up immediately.

Business impostor: A fraudster might contact you pretending to be from a well-known business. They might claim you've made a purchase that you didn't authorize and instruct you to call or follow a link to verify or dispute the purchase. If you're unsure whether the call is legitimate, look up the business's official phone number on its website and call the number directly. This scam might also involve fake notifications about undelivered packages.

Charitable scams: In this scam, someone pretends to be a charity and asks for a donation. Always inquire how much of your donation would actually go to the charity. Legitimate charitable organizations must register with the Ohio Attorney General's Office. You can verify a charity at https://charitable.ohioago.gov/Research-Charities. To ensure your donation goes to the right place, donate directly through the charity's official website or by calling a verified phone number. Be aware that scam charities often have similar sounding names to legitimate ones.

Ohio Turnpike Scam Alert

The Ohio Turnpike and Infrastructure Commission has reported a text message scam that fraudulently claims to represent tolling agencies across the country. Scammers request payment for unpaid tolls through fake websites. These messages are sent to random phone numbers, not tied to any specific account or toll road usage. Some recipients also reported receiving phishing emails. The Ohio Turnpike does not request E-ZPass payments via text, nor does it handle unpaid tolls through text messages. The only legitimate websites for Ohio Turnpike's E-ZPass accounts are ezpassoh.com and ohioturnpike.org.

For questions about the Ohio Turnpike's E-ZPass notifications, contact www.ezpassoh.com or www.ohioturnpike.org.

The FBI, aware of these impostor scams in several states, recommends the following actions if you receive a fraudulent message:

- Report the incident to the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov, and be sure to include:
    - The phone number from where the text originated.
    - Contact the tolling agency's customer service center.
- Delete any texts received.
- If you clicked any link or provided your information, make efforts to secure your personal information and financial accounts and dispute any unfamiliar charges.

In general, here are some red-flag requests that should warn you of a potential impostor scam:

- To wire money to a stranger or friend in need.
- To "act now!"
- To buy a prepaid money card.
- To send money in advance to secure or insure a loan.
- To provide personal information.

Consumers who believe they have been defrauded should immediately contact the company they used to make the payment. Ohioans can report scams to the Ohio Attorney General's Office at www.OhioProtects.org or by calling 800-282-0515.