Ohio Attorney General's Consumer Advocate Newsletter

Keeping Consumers Safe and Informed



December 2023



Winter-weather financial help in Ohio

For some Ohioans, winter fuels extra worry about personal budgets, what with higher heating bills and other expenses. From enhancing energy efficiency to selecting utility companies, the Ohio Attorney General's Office provides valuable seasonal tips to ensure safety, warmth and potential savings.

Utility disconnections

When electric and natural gas bills come in higher than expected, many people feel added stress. If you're struggling to pay your utility bills, you may be able to work out a payment plan with your local suppliers. Use the numbers on your monthly bill to inquire about a payment plan. Additionally, details on specific extended payment plans can be found <u>here</u>.

It's important to understand that you have <u>disconnection rights that must be honored before</u> <u>disconnection can take place</u>. Be sure to learn about Ohio's <u>Special Reconnection Order</u>, potentially reducing the cost of maintaining utility services in dropping temperatures.

Beware of scammers claiming that your overdue payments will soon lead to a loss of service. If contacted, request information that only an account representative should have, such as your address and account number. If the caller doesn't have this information, asks for personal details or insists on gift-card payments, it's likely a scam. Hang up and call your utility company directly using the number on your bill.

Wintertime energy savings and assistance efforts

To cut energy bills, consider getting a home-energy audit offered free (or for a moderate cost) by some local utility companies. Also, review this <u>online checklist</u> and <u>holiday energy savings tip sheet</u> to identify ways to use energy more efficiently. Explore <u>low-income assistance programs</u> such as the Home Energy Assistance Program (HEAP), which offers a one-time benefit for the winter heating season that is applied to electric, natural gas and/or bulk fuel bills. Individual utilities may have their own assistance programs.

In addition, be aware that certain governmental programs and grants are earmarked to help consumers pay their home energy bills and make improvements in energy efficiency. It's important to make sure that you work with a legitimate program, as scammers may try to pose as a governmental program. When seeking weatherization assistance, legitimate information is available at the <u>federal</u> and <u>state</u> levels. Suspected fraud, waste and abuse related to federal programs can be reported to the <u>U.S. Department of Energy's Office of Inspector General</u>.

Tips for propane consumers

In light of the supply-chain challenges and driver shortages of the recent past, propane users must prepare for the winter heating season. The Propane Education & Research Council and the Ohio Attorney General's Office offer these tips:

- Make sure that you have enough propane for winter. Never let the volume go below 25 percent without having placed a fill-up order with a propane supplier (the earlier, the better).
- If you run out of propane sooner than anticipated, call your supplier immediately so the supplier can inspect your system for potential leaks.
- Always be sure to have a clear path to your propane tank for easy delivery.

The Ohio Attorney General's Office can help with propane level emergencies, as the office prioritizes such cases.

Switching your energy supplier

Rising energy prices may attract competitive electric and natural gas suppliers, but savings are not guaranteed. Before switching, learn how to make <u>smart energy decisions</u> and <u>how to spot a utility</u> <u>scam</u>. Verify any "discount" or "rebate" offers from callers claiming to be your utility by contacting the utility directly using the number on your bill. Report potential scams to the <u>Ohio Attorney General's</u> <u>Office</u> and the <u>Public Utilities Commission of Ohio</u>.

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

Recurring subscriptions: Time for an assessment

With many Ohio families on a tight budget, the Ohio Attorney General's Office encourages consumers to review all recurring subscriptions and cancel any that are seldom or no longer used or no longer wanted.

The office suggests an audit based on the "three R's": Review, Reconsider and Remove.

- **Review your ongoing subscriptions.** Look at your subscription payments for various products and services by reviewing monthly credit-card, debit-card, and bank-account statements. Examples of potential ongoing charges include print and online magazines; streaming platforms for television, movies and music; product-of-the-month clubs (foods, coffees, teas, etc.); and mobile-device apps with monthly fees.
- **Reconsider your recurring charges.** Based on your review, discuss the needs and wants of your household. Identify products and services you're paying for that you rarely or never use and consider less-expensive options or scaled-down versions. Be skeptical. Ask whether you genuinely need a subscription service or can give it up to save money.
- **Remove subscription services you no longer want or need.** For subscriptions you plan to cancel, find out how to do so to avoid any future shipments and charges. Contact each company that bills your credit or debit card and state your decision. Keep copies of all documents and records of your communication with the company. If applicable, record the dates on which you mailed forms or letters rejecting future shipments.

Be sure to continue closely reviewing your credit-card and/or debit-card statements, looking for any charges you weren't expecting or charges for products or services you canceled.

If you find charges for products you didn't order, first try to resolve the problem with the company. If the company isn't responsive, contact your credit-card or debit-card company to dispute the charge. Ask the card company to reverse the charge because you didn't authorize the products or services.

Consumers who need help resolving a complaint against a business, or who suspect a scam or an unfair business practice, should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.

Scam trends: Older vs. younger victims

Although much attention is given to scams targeting older adults, recent statistics show that people of all ages are susceptible to certain types of scams. Surprisingly, some statistics show that younger populations are more likely to report scams even though older adults often experience higher financial losses.

According to the Federal Trade Commission (FTC), adults ages 18 to 59 are more likely to report losing money to scams, with online-shopping fraud, cryptocurrency investment scams and job scams being the most common. In 2021, the median loss for such scams was \$500.

Contrastingly, older adults (those 70 and older) were less likely to report fraud but tended to incur larger financial losses than younger victims. Older adults were more likely to fall pretty to tech-support scams and prize, lottery or sweepstakes scams, with a median loss of \$800 for those ages 70-79 and \$1,500 for those 80 and older.

Those under age 20 aren't immune from scammers, either, with data showing they are mainly targeted by scams involving peer-to-peer money transfers and online gaming.

Scam artists contact potential victims in many ways, including by email, phone call, text and socialmedia post.

Here's more information about some of the most common scams:

Online-shopping fraud: Such fraud typically involves a fake website selling items for an unusually low price. Shoppers might receive an email with a link to the fake site or click on an online advertisement that leads to the fake site. When the shopper attempts to buy items from the site, their money is collected but they won't receive the product. The shopper's credit-card information may also be compromised.

False cryptocurrency investment scams: An investment scam typically promises large returns with little investment. A popular version of the cryptocurrency investment scam includes false posts online that are promoted by celebrities and social-media influencers. The "celebrities/influencers" say they can multiply any amount of cryptocurrency you send them. If you send the cryptocurrency by clicking a link or through a QR code, the money goes directly to the scammers and will not be invested on your behalf.

Job scams: You may receive an email about or see a posting for a fake job. After you apply for the job and potentially give the "employer" your personal information, the scammers contact you with several next steps, including purchasing expensive software and materials for the job.

Typically, the scammers send you a check to supposedly cover the costs of the equipment and supplies. They persuade you to deposit the check into your bank account and then use a money-transfer service, gift card, or prepaid money card to send the same amount to a "vendor." After you send your real money to the "vendor," the check comes back from the bank as counterfeit and the bank retrieves the bogus funds from your account, plus often a bad-check fee and/or overdraft fees.

Be sure to research the company touted in any job posting before applying. If a job's pay rate doesn't seem to align with the skills necessary to do the job, it might be a scam.

Tech-support scams: A "computer company" – either by calling you or sending a pop-up message – claims that your computer has a virus. The scammer offers to fix the problem, then asks for access to your computer. Such access allows the scammer to install malicious software designed to scan your computer for personal information or to lock your computer, making it unusable until you pay a "ransom" to unlock it. Never allow remote access to your computer, and don't download or click on unfamiliar programs or files.

Prize, lottery or sweepstakes scams: With these scams, someone might falsely claim that you've won a lottery, prize or contest you didn't enter. To collect your "winnings," you are asked to pay a fee. Often, you are instructed to send money via wire transfer or money order, possibly to a foreign country. The scammer tells you to expect your winnings once you pay, but the prize never arrives. Be cautious of social-media "friends" or sweepstakes; such messages probably aren't from your friends.

Money transfer scams using peer-to-peer apps: Does your child or teen have a money-transfer app, such as Venmo or Cash App, on his/her phone? Scammers send users money, then text to claim the money was sent in error and ask the recipient to send it back. Only after sending the money does your child find out that the original payment didn't go through.

Online-gaming scams: As children make friends with other players online, they can be persuaded to share personal information, such as name, address and account password. Promises of free in-game currency, "skins" or other desirable gaming extras can persuade children to share payment information or click on links that lead to malware or spyware downloads.

Consumers who need help resolving a complaint against a business, or who suspect a scam or an unfair business practice, should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.

AG Yost's Meta lawsuit: Company harmed young users' mental health to boost profits

Ohio Attorney General Dave Yost and 32 of his counterparts nationwide have filed a <u>federal</u> <u>lawsuit</u> against Meta alleging that the social-media tech giant designed and deployed harmful features for Facebook and Instagram to addict young users to its platforms and enhance its bottom line.

The lawsuit, filed in U.S. District Court for the Northern District of California, claims that Meta concealed the severity of the psychological harm caused, including addiction to the platforms, which could, and in some cases did, result in physical harm.

"Given that children, when they're on these platforms, become vulnerable to cyberbullying and online predators, Meta has added insult to injury, further harming our children," Yost said. "I trust that the parents within Meta itself might reconsider these practices, but, until then, initiating lawsuits should compel the company to change its ways."

The federal lawsuit asserts that Meta violated state consumer protection laws by assuring the public that the platforms are safe and suitable for young users. Yet the company's practices harmed and continue to harm the mental and physical health of teenagers and pre-teens, the suit maintains, fueling what the U.S. Surgeon General has called a "<u>youth mental health crisis</u>," which has prompted suicides, devastated families and damaged a generation of young people.

The complaint further alleges that Meta violated federal law – specifically, the Children's Online Privacy Protection Act – when the company, aware that users younger than 13 were actively on its platforms, collected data from those users without parental consent. Meta targeted these youngest users after identifying them as a "valuable, but untapped" base, as reported in a 2021 <u>Wall Street</u> <u>Journal article</u>.

Meta's platform algorithms, the lawsuit says, push users into descending "rabbit holes," with the objective of keeping users on the platform for long periods. Meta also allegedly used features such as infinite scroll and near-constant alerts in a concerted effort to hold young users' attention. Such manipulative tactics entice teens and tweens to continually return to the platforms. Instead of disclosing the harm and making meaningful changes to minimize it, Meta publicly advertised their platforms as safe for young users.

The attorneys general also allege that the platforms served harmful content – including material associated with eating disorders, violence, negative self-perception and body-image issues, and bullying – to young users.

Simultaneously, the Ohio Legislature passed the Social Media Parental Notification Act, a new law designed to protect Ohio's children using social-media platforms. The law requires parental approval for children younger than 16 before creating new social-media accounts, ensuring parents receive notifications when their child opens a new social-media account.

Parents will be able to file complaints with the Ohio Attorney General's Office starting January 15, 2024. Stay tuned for more details on the filing process and other pertinent information.

SPOTLIGHT SERIES

Spotlight on...the Consumer Assistance Unit

The Consumer Assistance Unit of the Consumer Protection Section encompasses complaint specialists, the Identity Theft Unit and the Title Defect Recision Fund staff.

The team serves consumers, small businesses and nonprofits that file complaints against various businesses or who believe they are the victims of identity theft. In 2022, the Consumer Protection Section received nearly 23,000 complaints.

Complaint specialists play a crucial role, engaging with businesses to facilitate informal dispute resolution. They are trained to identify problems, and the complaint information they gather may be

referred for further investigation. Notably, many complaint referrals have resulted in successful litigation, showcasing the unit's contributions to addressing consumer concerns.

The Identity Theft Unit works with individuals to rectify the effects of identity theft. This involves contacting creditors, collectors, credit-reporting agencies and other relevant entities. Further, because children in the foster-care system may be especially vulnerable to identity theft, the unit works to correct errors that are discovered on the youth's credit reports.

Consumers who suspect an unfair business practice or who want help addressing a consumer problem should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.