Ohio Attorney General's
Consumer Advocate Newsletter
Keeping Consumers Safe and Informed

February 2026

Learn the benefits of filing your taxes early

Tax identity theft occurs when someone steals your personal information to file a fraudulent tax return and claim a refund. In recent years, concerns about identity theft have increased as data breaches have exposed Social Security numbers and other sensitive information. The sooner you file your returns, the less likely it is that someone can falsely file under your name.

In addition to ensuring that no one files taxes in your name, filing early may allow you to:

- **Get your refund sooner**: If you're expecting a refund, filing early usually means you get it sooner. E-filing with direct deposit typically results in refunds within 21 days; paper checks can take much longer.

- **Reduce stress and avoid last-minute rushing**: Tax season can be stressful, especially if you wait until April. Filing early eliminates the pressure of looming deadlines and gives you peace of mind.

- **Have more time to fix errors**: Starting early gives you extra time to review your return for accuracy, gather missing documents, and correct mistakes before the deadline. This can help you avoid penalties and ensure that you claim all eligible deductions and credits.

- **Protect against identity theft**: The risk of someone else filing in your name declines when you file early because your real return is already on file with the IRS.

- **Buy time if you owe taxes**: Even if you owe money, you will have time to budget and prepare for the payment if you file early. You can file in January but wait until the April 15 deadline to pay.

- **Enhance access to tax professionals**: Tax preparers get busier the closer the deadline gets. Early filing usually means quicker access to professional help if you need it.

Once you have decided to file your taxes early, you should get your documents organized. Make sure you have the following:

- **Personal information**: Social Security numbers (for you, your spouse and dependents), dates of birth for all household members, and bank account and routing numbers (for direct deposit).

- **Income documents**: W-2 forms from employers, 1099 forms (freelance, interest, dividends, retirement distributions), 1099-G (unemployment benefits), 1099-INT / 1099-DIV (interest and dividends), 1099-B (brokerage transactions), 1099-R (retirement income) and any other income statements (such as those for side jobs or rental income)

- **Deductions & credits**: Mortgage interest statement (Form 1098), property tax receipts, student loan interest statement (Form 1098-E), tuition statement (Form 1098-T), charitable donation receipts, child-care expenses (with provider details) and medical expenses (if itemizing).

- **Health coverage**: Form 1095-A, B, or C (proof of health insurance)

- **Other essentials:** Last year's tax return (for reference)**,** records of estimated tax payments (if any) and business expense records (if self-employed).

If you choose to use a tax preparer, follow these recommendations from the IRS.

If you suspect a scam or an unfair business practice, contact the Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Beware of Valentine's Day romance scams

If Valentine's Day has you eager to find someone special, be mindful of scammers who target people looking for love this time of year. Some con artists use dating sites and social media to build trust with victims before fabricating urgent financial needs. Common stories may involve a request for money to help pay for a plane ticket or for surgery suddenly needed by a family member. Always be cautious; never send money to someone you haven't met in person.

Romance scammers first work to build a strong emotional bond with victims through online communication, often portraying themselves as successful, wealthy and interested in a victim's life. Once victims invest a significant amount of money, scammers often become unresponsive, disappearing with the money and, in some cases, even blocking communication channels. Victims are left broken-hearted – and without their money.

Victims of romance scams don't fit a pattern; they may be male or female, young or old. The common denominator is that scammers prey on victims' belief in love.

Here are some examples of common romance scams:

- **Fake dating sites:** Victims are lured to fraudulent dating platforms that steal personal data or install malware.
- **Catfishing:** Scammers create fake profiles using stolen or AI-generated photos. They build trust over time, then ask for money or personal information. They often avoid video calls or in-person meetings.
- **Military romance:** This scammer pretends to be a soldier stationed overseas. He claims to need money for travel, a medical emergency, or a communication fee. This scam is among the most widespread and believable.
- **Fake investment opportunities:** The scammer poses as successful crypto trader or business mogul and promises huge returns if you invest. Instead, your money goes straight to the scammer.
- **Package or customs fees:** These scammers claim they've sent you a valuable gift, but say you need to pay a customs or shipping fee. The package never arrives.
- **Sextortion:** After gaining trust, these scammers persuade victims to share intimate photos. Scammers then threaten to expose these images unless victims pay them money. Reports of sextortion have surged, especially among younger users.

Here are some ways to avoid being scammed:

- Research people you meet online; do not rely solely on what they tell you. Conduct internet searches, including reverse-image searches, and check with independent sources to verify a person's claims. To do a reverse-image search, copy and paste the picture of the person you have been corresponding with into a search engine to see whether it is used on multiple accounts.

- Be cautious of “love bombing,” when a new love interest showers you with affection and compliments. Be cautious of individuals who claim that destiny or fate brought you together or claim to love you after only a short time.
- Be especially wary if you have just lost a loved one; many times, scammers study obituaries to find people who have recently suffered a loss, making them potentially more vulnerable.
- Be sure to talk to family members and friends about online relationships, even if the other person asks you to keep the relationship secret.
- Don’t send money to someone you have met only online, even if you have developed a relationship with the individual.
- Be very skeptical of requests for money to be sent via wire transfer, cryptocurrency, peer-to-peer payment systems (Venmo, Zelle, etc.), money order, prepaid money cards or gift cards. These methods of payment are preferred by scammers.

If you suspect a scam or an unfair business practice, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Ohio law provides protections for gym memberships

Have you joined a gym to help fulfill a New Year’s resolution for a healthier lifestyle? In Ohio, gym memberships are generally considered “prepaid entertainment contracts,” similar to agreements for dance or karate lessons or dating websites. These contracts provide consumers with certain rights, including the ability to cancel under certain circumstances.

Before signing a gym membership agreement, consumers should make sure that any benefits or features promised by the gym are included in the written contract. Only written promises are guaranteed. You should also carefully review the terms and conditions before signing, including any fine print.

Additionally, gym members should be aware of the following guidelines for canceling a prepaid entertainment contract:

- Consumers have three business days (excluding Sundays) to reconsider the purchase and cancel the agreement. The gym must provide customers a copy of the written contract containing a “notice of cancellation.”
- If a consumer cancels within the first three business days after entering into the prepaid entertainment contract, the gym must refund any money paid but may charge an expense fee no greater than $10.
- To cancel a gym membership, consumers should notify the gym by postal mail or in person. They should return the “notice of cancellation” provided with the written contract, or otherwise put the cancellation request in writing in the manner specified in the contract.

- If a consumer enters into a gym membership before the facility is doing business, the consumer has seven days to cancel from the first day the gym opens.
- If a customer moves 25 miles or more away from the gym, or if the gym relocates at least 25 miles away from a customer, the customer has the right to a refund based on the time remaining on the membership, unless a similar facility is located within 25 miles of the area of relocation.

Fitness centers that fail to give proper notice to consumers may be in violation of Ohio's consumer protection laws.

Before signing a contract, consumers who plan to join a gym should:

- Search for complaints on file with the Ohio Attorney General's Office and Better Business Bureau.
- Read the contract carefully and make sure verbal agreements are included in writing.
- Determine the total cost, including any extra fees for fitness classes or personal training.
- Find out whether payments will be withdrawn automatically from a bank account.
- Understand the cancellation policy and whether the contract renews automatically.
- Check the length of the contract, which should not exceed three years.

Joining a gym can be one of the first steps toward a healthier 2026. By applying the tips in this article, you will be better protected as you work toward your fitness goals.

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.

Basics about the national Do Not Call Registry

Placing a landline and/or cellphone number on the national Do Not Call Registry can help to reduce telemarketing calls, but it may not stop all unwanted calls.

Federal statutes require businesses to access the national Do Not Call Registry, maintained by the Federal Trade Commission, and to "scrub" – or remove – registered numbers from their calling lists.

Registration on the national Do Not Call Registry does not expire. Once your number is registered, it remains on the list unless you remove it. According to the Federal Trade Commission, more than 258 million phone numbers are registered as of September 2025.

The Do Not Call Registry does not include any automated call-blocking technology. Instead, businesses covered by the law are required to check the registry before making calls.
If you have registered and are still receiving unwanted calls, some may be from organizations exempt from the national Do Not Call Registry, including political groups, charities, debt collectors and survey

callers. In addition, companies with which you have an existing business relationship or that have your express written permission to call still may cause your phone to ring.

If you want to help limit these exempt calls, ask the caller to put your number on the organization's internal do-not-call list. Most legitimate organizations will have their own list, even if they are exempt from having to check the national Do Not Call Registry.

Consumers are often frustrated with the number of calls they get – most of the time, those calls are made by scammers. Scammers simply defy the Do Not Call law – and other consumer protection laws, for that matter. Do not respond to these calls; and, if you are on the Do Not Call Registry, consider it a red flag if you receive an unwanted call.

Those on the Do Not Call list who receive calls should take the following precautions:

- If you receive an unwanted robocall with an automated message, do not push any buttons – even to "talk to a representative" or "opt out" – because that may only confirm to the caller that your phone number is valid and working. And the result may be that, instead of getting fewer phone calls, you receive even more.

- If you receive multiple calls from the same phone number, call your phone provider for details about any available call-blocking features. In addition, third-party services may help to stop robocalls.

- Share your personal information – your name or phone number, for example – less often. Some companies may compile and sell your personal information. If a company requests such information, ask why the company needs it and how the company will protect it.

- Let unrecognized calls go to voicemail or to an answering machine that you monitor. When in doubt, just don't answer!

To sign up for the national Do Not Call Registry, visit www.donotcall.gov or call 888-382-1222 from the phone you wish to add to the nationwide list.

To report a scam, unfair business practice, or businesses not complying with the Do Not Call Registry, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.