Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

June 2025

Can you spot the signs of financial abuse against older adults?

Coinciding with Elder Abuse Awareness Day – on June 15 – the Consumer Protection Section of the Ohio Attorney General's Office is increasing their awareness efforts, educating Ohioans about the signs of financial abuse directed at senior citizens.

Financial abuse can be difficult to stop for many reasons. Victims may:

- Be reluctant to address the abuse due to their relationship to the abuser (who may be a friend or family member).
- Fear retaliation or shame.
- Depend on the abuser for assistance.

- Have health-related reasons (physical or emotional) or economic reasons for not reporting the abuse.

The financial abuse is commonly committed by:

- Family members, friends, neighbors or acquaintances.
- Professionals (such as attorneys, doctors, financial advisers, clergy members, caregivers or guardians).
  Strangers (such as telemarketers, door-to-door salespeople, romance scammers or fake media personalities).

Indicators of financial abuse include:

- Fraudulent signatures on financial documents.
- Unpaid bills.
- Sudden changes in spending habits, wills or other financial documents.

To help prevent financial abuse, older adults are encouraged to:

- Plan ahead for legal, medical and estate matters.
- Seek independent advice from someone you trust before signing any documents. If you don't understand a financial transaction or think you're being pressured to give money and/or sign a document, ask for help.
- Avoid sharing personal information with people you do not know well.
- Make sure that proper screening and background checks are completed before hiring someone to provide services.

The attorney general's Consumer Protection Section encourages all older adults to

ALWAYS:

- Be skeptical when someone requests immediate payment via wire transfer, prepaid money card, gift card, cryptocurrency or a peer-to-peer payment network.
- Research businesses and charities through the Ohio Attorney General's Office and the Better Business Bureau.
- Beware of strangers who seek new, quick personal connections with you or a loved one.
- Get all verbal promises in writing and review all contracts.
- Keep your personal information private and shred outdated documents containing such information.

NEVER:

- Send money to a stranger via wire transfer, gift card or prepaid credit card.
- Give personal information to someone who has contacted you unexpectedly.
- Carry unnecessary personal information, such as your Social Security card, in your wallet or purse.
- Pay to win a prize or sweepstakes.
- Give anyone "remote access" to your computer.
- Pay the full amount before any work has been done.
- Sign documents you don't understand.

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

Cryptocurrency-related scams: What to do after a financial loss

With today's economic uncertainty and increasing media coverage of cryptocurrency, some consumers are falling victim to investment scams and other cons involving one or more types of digital money.

Cryptocurrency, often called *crypto*, is not government-backed; it can be highly volatile and risky.

Common types of crypto include Bitcoin, Ethereum, Binance and Ripple. Scammers like to request crypto because it lacks many of the same protections that other payment forms provide and is hard to trace once the money is sent.

If you've fallen victim to a cryptocurrency-related scam, the federal Commodity Futures Trading Commission (CFTC) suggests taking these six steps:

1) Stop sending crypto. If you've already sent cryptocurrency to a scammer, the scam might not end there. For example, the scammer – posting as a government official, a recovery company or an attorney – may suggest that, for a fee, he/she will get your lost funds back. This is never true; it's part of a recovery scam to simply steal additional money from victims.
2) Gather documentation. Be sure to write down all the scam details that you recall, including conversations you had and the date/time of these calls, chats or messages. Be sure to save any website addresses, screenshots, phone numbers, email messages and email addresses as well as any receipts or statements of any payment types you used to pay the scammer (credit cards, crypto, money transfers, prepaid money cards, etc.).
3) Protect your identity and financial accounts. If the scammers have your payment information, take action to block their access to your accounts. If you gave out your personal information, such as a Social Security number, consider putting a fraud alert or security freeze on your credit reports by contacting the three major credit reporting agencies (Equifax, Experian and TransUnion). Fraud alerts and credit report freezes are free and do not affect your credit score.
4) Report the scam to relevant authorities. These authorities may include state agencies (such as the Ohio Attorney General's Office and the Ohio Department of Commerce's Division of Securities), federal agencies (such as the CFTC and the U.S. Department of Justice) and local authorities (such as a local police department or sheriff's office).
5) Begin seeking financial recovery. Review your homeowner's insurance policy for fraud loss and/or identity-theft protection. Speak with a tax professional to find out about any opportunities to claim financial losses if you itemize your deductions. Talk with a reputable financial adviser and/or nonprofit credit-counseling organization about how to help repair any debt and deal with financial losses.
6) Reflect on what led to the scam. The CFTC says: "Routine activities can lead people to becoming targets, and returning to those activities could start the process all over again. These routine activities could include being active in investor social-media groups or chat rooms, commenting on videos, signing up for trading courses, special offers, free giveaways, or investor newsletters."

It's important to stay vigilant and to recognize that once a scammer has stolen funds, your personal information may be sold to other scammers on the dark web. Be sure to keep your guard up and especially watch out for recovery fraudsters seeking to gain access to more of your money under the guise of helping to recover lost funds.

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.

Keep your guard up for phony government licenses and credentials

Some regulatory agencies, boards and commissions are reporting that credentials for their regulated professions are being forged or even stolen.

For example, the Ohio Architects Board has noticed individuals offering design services while falsely claiming to be licensed. In some cases, a customer has paid for official-looking stamped or sealed building plans, only to learn from their local building department, after submitting the plan for approval, that the seal is fake. The victim is stuck with a useless plan as well as lost time, effort and money.

Unfortunately, Ohio's architecture community is not alone. The Ohio Architects Board reports that other states and other professions are also seeing fraudsters presenting themselves as licensed professionals.

What can consumers do?

It is important for Ohioans to educate themselves about which professions are regulated and at what level of government (local, state or federal). It's equally vital that consumers learn which professions are *not* regulated, so they don't accept a phony license at face value.

Within Ohio's state government, click here to learn more about how certain professions are regulated and by whom. For example, besides architects, Ohio regulates various other professions and trades, including accountants, barbers, engineers, lawyers, nurses and physical therapists. You can learn about licensure in many of these professions through an online search of the relevant board, commission or agency website.

More than 20 Ohio agencies, boards and commissions can be researched using the eLicense Ohio Professional Licensure System. These entities typically can provide a roster of licensees in Ohio and any disciplinary action that has been taken against a regulated business or individual. Other state regulatory agencies and organizations that issue credentials may have online search tools available directly through their official websites.

As for professions and trades that are *not* currently regulated at the state level, have you ever heard of a state-certified cabinet installer or state-approved roofer? Hopefully not, because credentials at the state level don't exist in Ohio at this time (but keep in mind that state laws, rules and policies can change). Although a roofing contractor needs to be registered with the Ohio Secretary of State's Office, Ohio does not license roofers. Some municipalities or other local jurisdictions, however, may have laws or rules requiring registration or other actions before doing certain work within their boundaries.

Tips to avoid being scammed by an impostor:

- Verify any credentials touted by a business or contractor. If someone claims to be licensed or registered with a specific professional organization, trade association or government regulator, check it out. Find out first what licenses and/or registrations apply to the particular trade or service. Then check out any specific registrations or licenses by contacting the entity that the business purports to be accredited by.
- If a prospective contractor in a regulated profession refuses to give his/her license number or credentials before entering into a contract or will disclose it only after payment is made, the person is probably a scammer.
- Take note if the regulator's contact information for a certain business (i.e. email address, phone number, etc.) differs from what your contact at the business has given you. The real business may be a victim of impersonation by someone without a license.
- Get recommendations and ask a business for references. Successful contractors make it easy to access feedback about their work and related documentation.
- Go online to research the business. Check out whether the company has been the subject of complaints at the Ohio Attorney General's Office and the Better Business Bureau. You can also search for any previous lawsuits filed by the attorney general's Consumer Protection Section.

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.

Artificial intelligence is being used in consumer scams

Businesses and organizations are increasingly using artificial intelligence when communicating with their customers. But scammers, too, are using AI – to *deceive* consumers.

Legitimate customer service departments use AI chatbots to increase the efficiency of communication with customers in real time. Scammers, in turn, create fake chatbots to ask customers for payment information and personal identifiable information. These fake chatbots direct users to a fake website.

To protect yourself while interacting with a chatbot, be sure to:

- Verify the source. If you encounter the chatbot as a pop-up while not visiting that company's website, do not click on the chatbot. Visit the company's official website to interact with its chatbot.

- Take your time. Scammers use a sense of urgency to force victims into a quick decision. Don't let yourself be rushed.
- Keep your personal information private. Legitimate company chatbots will never ask for account passwords or Social Security numbers over chat.

Phishing emails are correspondence that look as if they're from a legitimate company, with some even including the company's logo and links to their website that prove to be fraudulent. Phishing emails are not new, but the use of AI technology has improved the quality of these scam emails.

When you receive a suspicious email be sure to check:

- Email addresses. Hover above the sender's email address with your cursor. If the email address differs from what you know or would imagine to be a legitimate email address, it may be a phishing attempt. Find an email address for the company you know to be legitimate – on a past bill or the company's official website.
- Links. Avoid clicking on links in the body of an email; doing so may direct you to a website designed to steal your money or personal information.
- Attachments. Do not click on any attachments before verifying that the email sender is legitimate. Attachments may contain malware designed to harm your device.

Misinformation campaigns use AI technology in the form of fake videos and audio campaigns to impersonate a family member, business or celebrity. For example, you might receive a phone call from someone who sounds like a relative or see a video post of a celebrity on social media. The key to identifying these scams is to evaluate what you're seeing or hearing and deciding whether the message from that person is reasonable.

Here are some techniques to do that:

- Use verification methods. One step may be to use a "password" for family members to request money in an emergency.
- Take a close look. When viewing an online video, check for imperfections and glitches.
- Check facts. If the request or promotion comes from a business or celebrity, do a quick internet search to see whether the business or celebrity is really associated with that product or promotion.

AI-generated scams use elements of traditional scams with improved application. If you think you have interacted with any of the above scam techniques:

- Check your credit report for any unknown accounts.
- Communicate with your financial institutions regarding potential fraud.
- Change any account passwords associated with the account where the correspondence was received.

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

BONUS TIP YOU CAN USE: If you are turning to social media to resolve an issue with a business, proceed cautiously. According to an alert from the Better Business Bureau, scammers are known to respond to such public requests for help by creating phony accounts and contacting consumers posing as the business to try to steal personal and financial information. Check out all the details, including tips to avoid this type of impostor scam, by reviewing this alert.

OHIO SALES TAX HOLIDAY – GOOD NEWS TO KNOW

This year, the sales-tax holiday will last 14 days – from **Friday Aug. 1 through Thursday Aug. 14**. The event permits tax-free purchases online and in person on all eligible items totaling up to $500 per item.

Although traditionally associated with back-to-school purchases and school supplies, nearly all other items are eligible for the tax exemption. General exceptions include services, boats, automobiles, liquor, tobacco, vapor products and items containing marijuana.

When shopping, make sure you understand which items are eligible for the exemption. Also, practice sound shopping habits, such as keeping receipts and knowing the return policies of the stores where you shop.

The Ohio Department of Taxation provides detailed information about the expanded sales-tax holiday. Before heading out, consider the types of purchases you plan to make and review the Ohio Department of Taxation's Sales Tax Holiday webpage.

For questions about the Ohio Sales Tax Holiday, call the Department of Taxation at 1-888-405-4039.