FLORIDA CONSUMER
# NEWSLETTER
January 2026
A publication of the Florida Department of Agriculture and Consumer Services

# NEW YEAR, NEW GYM MEMBERSHIP

Happy New Year! If you are just beginning the journey to a healthier you due to a resolution you made, congratulations! If you are determined to find just the right place to work out, then read on to learn how you can protect yourself when it comes to gym membership.

Signing up for a gym sounds easy and some even offer free trials. However, the Better Business Bureau warns not to share your bank account or credit card information when you sign up for that free trial. Many gyms will automatically begin to charge a membership fee if you forget to cancel your "membership." Make sure you understand all terms and conditions of the free trial and that any commitment ends in a specified time frame.

Let's say you have found the perfect gym and signed the contract but then decide it is not the place for you. You thought cancelling would be easy – just go online and select "cancel." The process is not quite that straightforward at some gyms; in fact, it could be quite challenging to cancel. For example, the Federal Trade Commission alleges that LA Fitness made it nearly impossible for their customers to cancel their contract, costing excess time and money for those who wanted out.

Consumers are encouraged to do some research in advance of selecting a gym to ensure there are no problems when the time comes to move on from the membership.

- **Check online reviews.** Search for the name of the gym and the word "subscription" or "contract" plus words such as "complaint," "problem," "cancel," and "fee." Read through the results to get an idea of how easy or difficult it is to end a relationship with the gym.
- **Read the fine print.** We all know to do this when buying a house or a car or other big ticket item but may not think it applies to gym membership. It certainly does! Does the membership renew automatically? How are you notified of price changes? What do you have to do to cancel?
- **Ask questions.** Have the staff spell out what is included in the membership and what is not. Ask specifically about renewal and cancellation.

If you already have a membership and have tried to cancel, yet they just keep charging your card, contact your bank to dispute the charges and block future charges. It's a sure thing your contract will be quickly cancelled.

Under Florida's Health Studio Act, health studios (gyms) are required to register with the Florida Department of Agriculture and Consumer Services (FDACS). In addition, some health studios must post security for a limited time. By requiring health studios to provide a bond or other financial security, FDACS can provide some financial protection to members of a health studio that closes unexpectedly. The funds can then be used to compensate members who purchase long-term contracts. Read more about your rights and how to protect yourself on our website. To make sure the gym you choose is registered, visit Business Search. If you have a complaint about a health studio, use our online complaint form or call 1-800-HELP-FLA (435-7352).

# IS THAT VIDEO REAL OR NOT?

In our continuing discussion on artificial intelligence, or AI, this month we will cover videos created using artificial intelligence. These videos are commonly known as deepfakes; the definition of deepfakes includes images or sound in which a person's face, body, or voice has been digitally altered and are often used maliciously or to spread false information. According to research from the digital identity firm Signicat, deepfakes have surged by over 2,100% since generative AI went mainstream in 2022. For the purposes of this article, we will be covering deepfake videos.

## EXAMPLES OF DEEPFAKE VIDEOS

Do you remember when video evidence was incontrovertible proof of what was shown on the video? Video proof can no longer be used as stand-alone evidence due to deepfakes; videos are supportive along with witness testimony and other accompanying evidence. There are many forms of deepfake videos, as noted in the list below and how those can be used.

**Face-Swap Deepfakes:** These videos overlay the face of one person onto the body of another body in motion. The AI neural networks are adept at matching expressions frame by frame with the body in motion, creating realistic looking video. Some of these deepfakes are just for fun, but others can be used for malicious purposes, like ruining a reputation or spreading false information.

**Lip-Syncing and Audio Overlays:** Sometimes called puppeteering, lip-sync deepfakes rearrange mouth movements to match audio, which may be manipulated or completely synthesized. Combined with voice cloning, which we covered last month, the "person" on the video appears to speak but the words were never spoken by any person.

**Full-Body Reenactment:** These videos feature models generated completely by AI, encapsulating one actor's posture, mannerisms, and movement, and ascribing those to a different individual. These deepfakes feature a person or people who appear to be performing tasks or involved in activities which they never did. Although movies and television use this in filming, the malevolent use is that of staged evidence and bogus alibi videos.

## SCAMS USING DEEPFAKE VIDEOS

**Investment Scams:** Watch out for investment requests from your favorite stars. Scammers create deepfake videos, employing the likenesses of financial gurus or celebrities urging viewers to invest in phony schemes, or “exclusive” deals. After the money is sent or the personal information is provided, the scammer can no longer be found, with no return for the victim. An example is a recent scam involving the “CEO” of a crypto company. A video the recruit investors featuring the “CEO” was actually an avatar reciting a script, all programmed with AI.

**Romance Scams:** Use caution when looking for a relationship online. If you meet someone who seems charming and too good to be true, they may be. After creating fake accounts, the scammer uses AI to generate photos, videos and even video chats that may be deepfakes to build relationships. After gaining the trust of their victim, the scammer begins to ask for money or personal financial information.

**Fraud:** Scammers are using AI deepfakes to commit fraud on social media. By manipulating video and audio of content creators, they create new content that appears to be the original creator selling a (non-existent) product for a (bogus) cause. The deepfake videos target the creator’s following or audience.

Among the most deepfaked celebrities is Taylor Swift, who “appeared” in a series of social media ads offering free Le Creuset cookware. Participants only had to provide their personal information and pay for shipping. Unfortunately, the videos were fake, and she never made such an offer. Scammers scored the financial and personal information of thousands of Swifties, in addition to the cash.

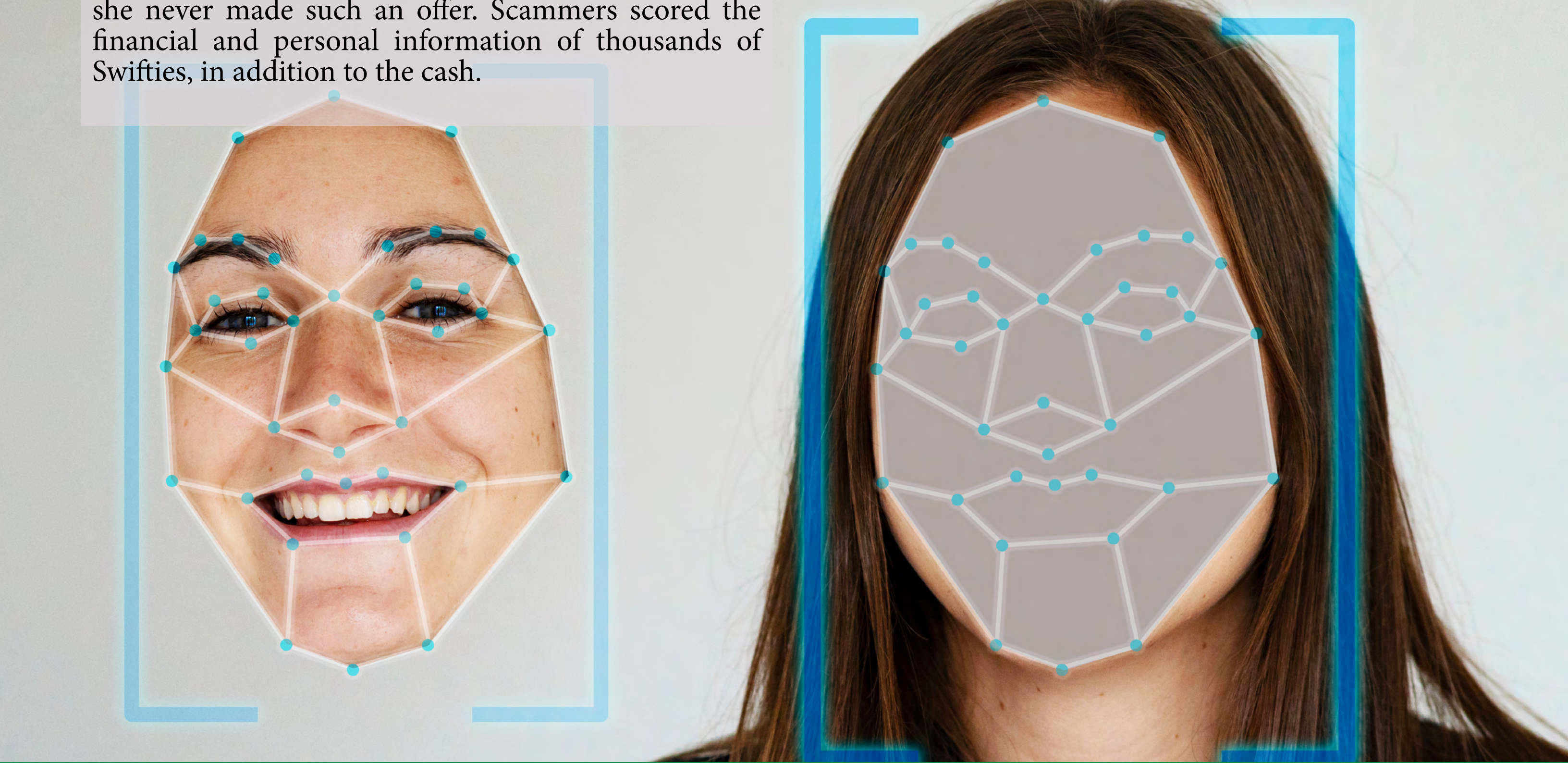
## DETECTING DEEPFAKES

How can you, the layperson, determine if a video is a deepfake? Here are a few examples you can employ without having to purchase extensive digital equipment.

**Human observation:** Your first line of defense in determining if a video is a deepfake is by watching closely. Look for clues that the figure in the video is an illusion, such as unnatural actions, facial features in which the expression is mismatched or distorted, and inconsistent movement. Do the hair and teeth look real? Are the eye movements natural? Pay attention to subtle anomalies in skin texture, blinking patterns, or mismatched reflections.

**Context cues:** Consider the background in the video. Are there no shadows when there should be? Or are the shadows not consistent with the lighting? Notice if the audio and video are out of sync. If there are objects moving, does the movement make sense?

**Cross Reference the Source:** If you see a suspicious video clip indicating the presence of someone, check the official source of the location to prove or disprove the claim. Press releases often contain alternative camera angles to prove such claims. Mainstream media relies on such cross-checks in the name of credibility.



# KIDNAPPING SCAMS

On December 5, 2025, the Federal Bureau of Investigation (FBI) issued an announcement warning the public of scammers who find and alter photos found on public websites and social media for use in virtual kidnapping scams. These bad actors stage a fake kidnapping then demand a ransom.

**Contact from the "Kidnapper"**

The criminals in this scam usually contact their victims by sending a text message, also known as smishing, claiming to have kidnapped a family member or loved one to extort money from the victim. In this text exchange, the "kidnapper" will threaten significant acts of violence if the demands for ransom are not met immediately and follows up with photos or videos of the loved one. These photos are scheduled so the victim does not have time to scrutinize the images and confirm the authenticity. Upon close inspection, the images may have odd proportions, or verifiable details may be missing, such as scars or tattoos. The original photos have been altered to fit the narrative of the scammer, so it could be a familiar photo, cropped, with an added background or other features.

**Protect Yourself**

- Agree on a code word that only you and your loved ones know to verify communication.
- Share pictures of your family and yourself only with those you know, not with the public. Facebook's privacy settings let you limit who can see your posts and profile information.
- When traveling, do not provide personal information to strangers and wait until you return home to post those beautiful vacation photos.
- If you post missing person information online, be wary of information provided by strangers, as it might be a scam.

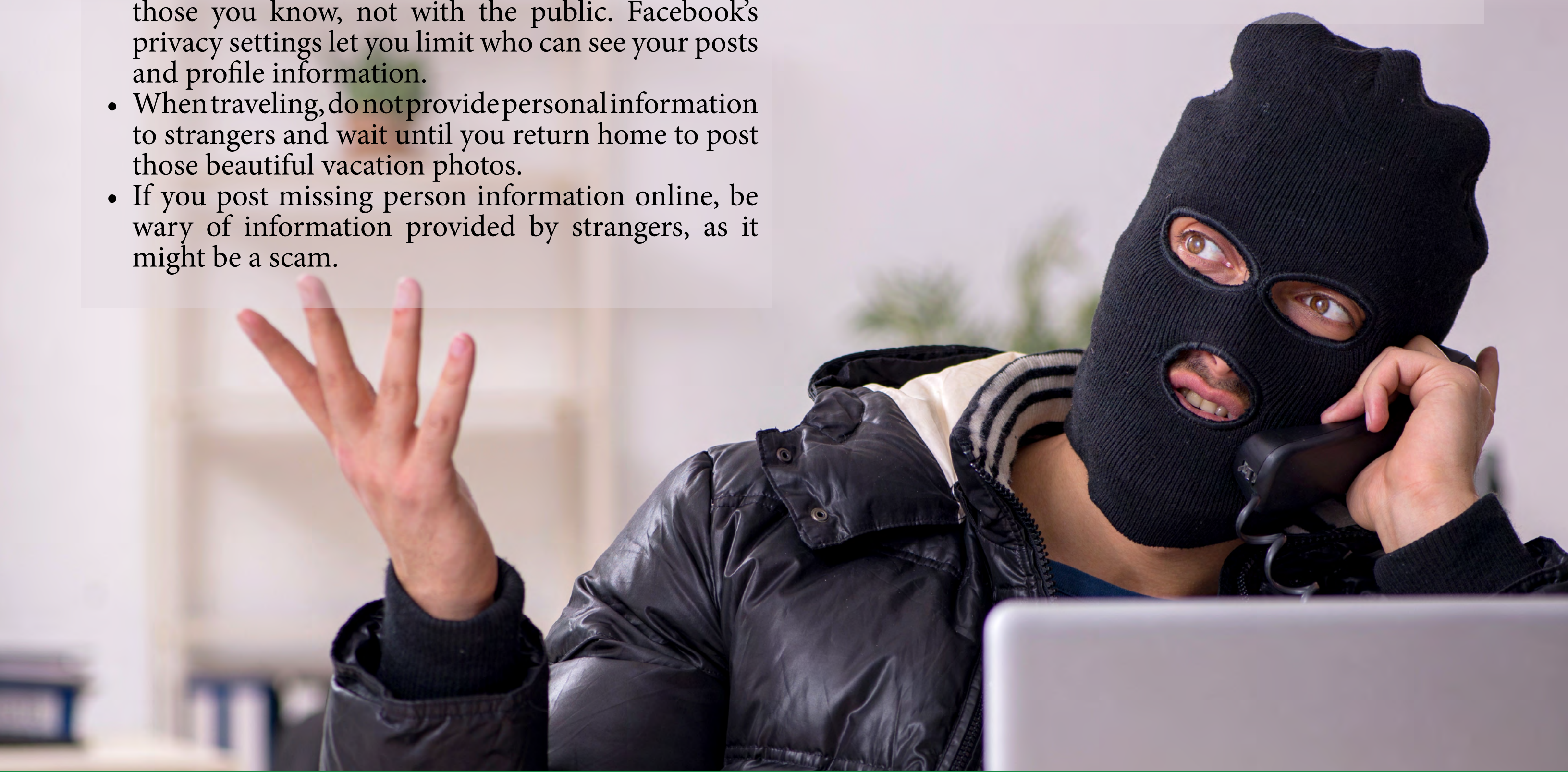
If you receive a message claiming a loved one has been kidnapped and demanding a ransom,

- Don't react to a false sense of urgency. Take the time to process what is happening.
- Consider the kidnappers claim – does it make sense?
- Screenshot or record proof of life photos whenever possible.
- Always attempt to contact your loved one before considering paying the ransom.

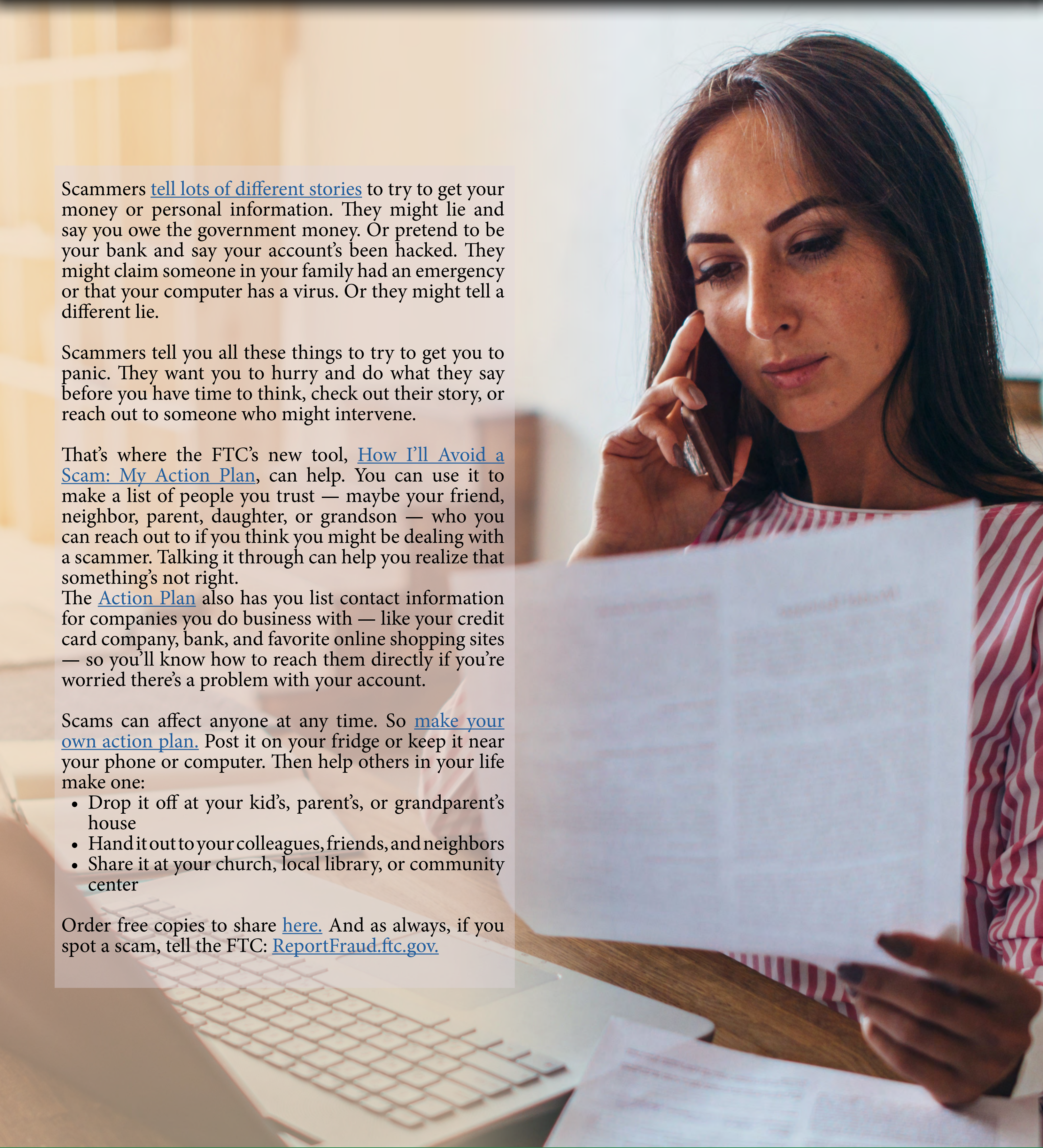
In a second warning on December 8, the FBI again warned the public of the danger of scams. "If you feel pressured to act fast, pay money, or turn over personal information—take a beat. Stop and assess if what you're being told is real. Talk to your families. Protect each other from scams," said FBI Director Kash Patel. "Scammers are banking on the fact that you'll feel too embarrassed to come forward and report the crime to the FBI. Don't let them win."

**Report It**

If you are a victim of a virtual kidnapping scam, report the incident to the FBI's Internet Crime Complaint Center at www.ic3.gov. Be sure to submit as much information as possible about the interaction including phone numbers, payment information, text and audio communications, and proof of life photos. Keeping records of all information is helpful in an investigation.



# USE THIS ACTION PLAN TO AVOID SCAMS



Scammers tell lots of different stories to try to get your money or personal information. They might lie and say you owe the government money. Or pretend to be your bank and say your account's been hacked. They might claim someone in your family had an emergency or that your computer has a virus. Or they might tell a different lie.

Scammers tell you all these things to try to get you to panic. They want you to hurry and do what they say before you have time to think, check out their story, or reach out to someone who might intervene.

That's where the FTC's new tool, How I'll Avoid a Scam: My Action Plan, can help. You can use it to make a list of people you trust — maybe your friend, neighbor, parent, daughter, or grandson — who you can reach out to if you think you might be dealing with a scammer. Talking it through can help you realize that something's not right.
The Action Plan also has you list contact information for companies you do business with — like your credit card company, bank, and favorite online shopping sites — so you'll know how to reach them directly if you're worried there's a problem with your account.

Scams can affect anyone at any time. So make your own action plan. Post it on your fridge or keep it near your phone or computer. Then help others in your life make one:

- Drop it off at your kid's, parent's, or grandparent's house
- Hand it out to your colleagues, friends, and neighbors
- Share it at your church, local library, or community center

Order free copies to share here. And as always, if you spot a scam, tell the FTC: ReportFraud.ftc.gov.

# ABOUT THE FDACS DIVISION OF CONSUMER SERVICES

FDACS is Florida's state consumer protection agency responsible for regulating charities and handling consumer complaints. FDACS handles more than 400,000 consumer complaints and inquiries, oversees more than 500,000 regulated devices, entities, and products like gas pumps and grocery scales, performs over 61,000 lab analyses on products like gasoline and brake fluid, performs nearly 9,000 fair ride inspections, and returned over $2.8 million to consumers through mediations with businesses.



The Division of Food Safety monitors food from the point of manufacturing and distribution through wholesale and retail sales to ensure the public of safe, wholesome and properly represented food products.

**CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.**


The Consumer Product Safety Commission provides consumer product recall information as part of the agency's mission to protect consumers and families from hazardous products.

**CLICK THE ICON ABOVE TO SEE THE LATEST RECALLS, MARKET WITHDRAWALS, & SAFETY ALERTS.**

*The Florida Department of Agriculture and Consumer Services is the state's clearinghouse for consumer complaints, protection and information. Consumers who would like information about filing a complaint against a business or who believe fraud has taken place can visit us online at [FloridaConsumerHelp.com](FloridaConsumerHelp.com) or contact the department's consumer protection and information hotline by calling 1-800-HELP-FLA (435-7352) or 1-800-FL-AYUDA (352-9832) for Spanish speakers.*