FLORIDA CONSUMER NEWSLETTER

April 2025

A publication of the Florida Department of Agriculture and Consumer Services

APRIL IS NATIONAL CAR CARE MONTH

There are over 18 million registered vehicles in Florida, and those vehicles represent a significant investment for Florida consumers. Taking care of any vehicle-related issues is important for your safety and the longevity of your vehicle. However, it is equally important to ensure that service and repairs are provided by a properly licensed motor vehicle repair shop.

The Florida Motor Vehicle Repair Act requires anyone in Florida, who is paid to repair motor vehicles owned by other individuals, to register with the Florida Department of Agriculture and Consumer Services (FDACS). Before engaging in services with a motor vehicle repair shop, use the "Business License Lookup" feature at FloridaConsumerHelp.com to ensure the business is properly licensed.

Start shopping for a repair shop before you actually need one. You will be more likely to make a better decision if you are not rushed or in a panic. When you do select a business, make sure they will honor your vehicle's warranty, if applicable. It's always a good idea to ask friends and associates for their recommendations.

Ask how the shop prices are estimated before you arrange to have any repairs made. Some shops charge a flat rate for labor on repairs while others may charge for labor based on the type of work performed. If the repair work will cost more than $150, the repair shop MUST give you the option to request a written estimate, to be notified by the shop if the repair exceeds an amount you specify, or to not require a written estimate at all. Motor vehicle repair shops cannot force you to waive your right to an estimate.

Do not choose a motor vehicle repair shop just because they offer the least expensive repair. Saving a few dollars and not having your vehicle repaired properly may end up costing you more in the long run. If you are unsure that you need a specific repair, don't be afraid to get a second opinion.

The Florida Department of Agriculture and Consumer Services is the state's clearinghouse for consumer complaints, protection and information. If you need to file a complaint about a motor vehicle repair shop, contact the FDACS Consumer Assistance Center at 1-800-HELP-FLA (435-7352) or, for Spanish speakers, 1-800-FL-AYUDA (352-9832) or visit File a Complaint. For more information on motor vehicle repair shops, visit Consumer Rights and Responsibilities/Motor Vehicle Repair at FloridaConsumerHelp.com.

CHECK WASHING

The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, has identified check fraud as the largest source of illicit proceeds in the United States. Bank Secrecy Act reporting for check fraud has increased significantly in the last few years, with financial institutions filing more Suspicious Activity Reports (SARs) to FinCEN. The Bank Secrecy Act of 1970, also known as the Currency and Foreign Transactions Reporting Act, is a U.S. law requiring financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering.

Despite the declining use of checks in the United States, criminals have been increasingly targeting the U.S. Mail to commit check fraud since the COVID-19 pandemic. Criminals committing this type of mail theft-related check fraud generally steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits.

The United States Postal Inspection Service (USPIS) has reported that mail theft-related check fraud is increasingly committed by scammers ranging from individual fraudsters to organized criminal groups comprised of the organizers of the criminal scheme, recruiters, check washers, and money mules. These criminals target USPS blue collection boxes, unsecured residential mailboxes, and privately owned cluster box units at apartment complexes, planned neighborhoods, and high-density commercial buildings.

Money Mule: a person (whether witting or unwitting) who transfers or moves illicit funds at the direction of or on behalf of another.

Fraudsters alter or "wash" the checks, replacing the payee information with their own or fraudulent identities or with business accounts that the criminals control. They will often increase the dollar amount on the check, sometimes by hundreds or thousands of dollars. Washed checks may also be copied, printed, and sold to third-party fraudsters on the dark web and encrypted social media platforms in exchange for convertible virtual currency. In some cases, victim checks are also counterfeited using routing and account information from the original, stolen check.

Check Washing: the use of chemicals to remove the original ink on a check to replace the payee and often the dollar amount. Fraudsters may also copy and print multiple washed checks for future use or to sell to third-party criminals.

In many cases, the criminals may cash or deposit checks in person at financial institutions, through automated teller machines (ATMs), or via remote deposit into accounts they control, and which they often open specifically for the check fraud schemes. They may also utilize money mules and their pre-existing accounts to deposit fraudulent checks. Regardless, once the checks are deposited, the fraudsters often rapidly withdraw the funds through ATMs or wire them to other accounts that they control to further complicate the money trail. Following the initial theft and fraudulent negotiation of the stolen checks, criminals may continue to exploit their victims by using the personal identifiable information found in the stolen mail for future fraud schemes, such as credit card fraud or credit account fraud.

CHECK WASHING: PROTECT YOURSELF

Postal Inspectors recover more than $1 billion in counterfeit checks and money orders every year, but you can take steps to protect yourself.

- **Use indelible black gel ink pens when writing checks.** Because of its chemical properties, indelible ink may resist a scammer's typical washing mixture, which can include acetone, bleach, and rubbing alcohol.
- **Use checks with one or more security features.** Check manufacturers add specific hallmarks to checks to reduce the chances of fraud. Talk to your bank to confirm that your checks have some of these features such as watermarks, copy void pantographs, security ink, visible or invisible fibers, three-dimensional reflective holostripe, and high-resolution micro printing.
- **Don't put checks in your home mailbox for pickup.** The little flag that alerts your mail carrier may also signal potential thieves that there's something inside.
- **Deposit mail before last pickup.** Avoid leaving checks in blue collection boxes overnight, as they are more vulnerable to theft.
- **Retrieve mail frequently.** Never leave your mail in your mailbox overnight.
- **Hold mail at Post Office.** If you're going on vacation, have your mail held at the Post Office or have it picked up by a neighbor, friend, or relative.
- **Use electronic payment methods:** Whenever possible, opt for electronic bill pay or transfers instead of mailing checks.
- **Monitor your bank account online regularly.** Confirm the checks that have been cashed and report anything that seems suspicious.
- **Report any suspicious activity to your bank:** If you suspect your checks have been stolen or altered, report it to your bank immediately.

If you believe you have been a victim of mail theft-related check fraud, promptly contact your financial institution and report it to the USPIS at 1-877-876-2455 or https://www.uspis.gov/report.

BEWARE OF MFA FATIGUE

Multi-Factor Authentication (MFA) is a crucial security measure that provides an extra layer of protection to your accounts. Even if a cybercriminal manages to steal your username and password, MFA makes it significantly more difficult for them to gain access. Unfortunately, cybercriminals have developed tactics to manipulate people into approving malicious login requests.

MFA fatigue, also known as MFA bombing or MFA exhaustion, is a cyberattack that involves sending repeated requests for MFA to a victim. The goal is to trick the victim into approving a request, which would give the attacker access to the victim's account. By sending repeated MFA prompts, cybercriminals can capitalize when people get distracted, frustrated, or mistakenly approve a fraudulent MFA prompt. When this happens, the attacker can compromise the extra layer of security and gain access to your account.

Your awareness is the first and best line of defense against cyber threats. ALWAYS THINK, BEFORE YOU CLICK! Keep your accounts secure by never approving the following MFA prompts…

- **Unexpected MFA prompts:** Prompts that pop-up while you are already logged in to an account or at an unusual time or prompts that you did not initiate. If you receive an unexpected MFA prompt, consider it suspicious and do not approve it!
- **MFA prompts that come after opening a suspicious message:** If you recently received a phishing email or clicked a linked that asked for your credentials—do not approve the MFA request! Reset your password and report it immediately!
- **Multiple MFA prompts in a row:** If you receive multiple, back-to-back MFA prompts, it might be an attacker using the MFA fatigue tactic do not approve them!
- **MFA prompt from unknown locations or unknown devices:** If you get an MFA request from an unfamiliar location or unknown device—do not approve it—legitimate login attempts originate from your device and location.
- **Phone calls or text messages asking you to approve an MFA prompt:** Scammers impersonating IT support may call and ask you to approve an MFA prompt. Do not approve the prompt, reset your password, and report it immediately.
- **Unknown Sign-In pages:** Do not enter your account credentials into unknown, unauthorized, or unexpected Sign-In pages.

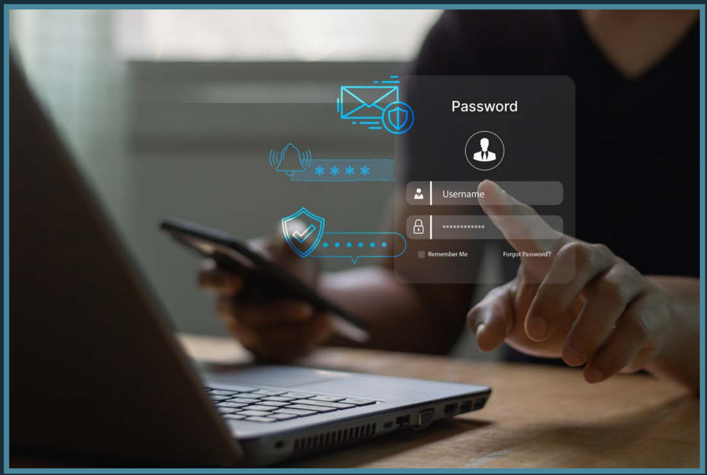
Pro Tip: If you experience frequent, unauthorized MFA prompts, enable number-matching or biometric authentication instead of push notifications to improve security.

Number matching is a setting that forces you to enter numbers from the identity platform into your app to approve an authentication request. The number matching requirement mitigates MFA fatigue by:

- Requiring access to the login screen to approve requests. Users cannot approve requests without entering the numbers on the login screen.
- Discouraging prompt spam. Each prompt generates a unique set of numbers for every login request. As the user cannot accept the prompts without knowing the numbers, generating multiple prompts is not effective.

Biometric authentication refers to a cybersecurity process that verifies your identity using your unique biological traits such as fingerprints, voices, retinas, and facial features.

Report Suspicious Email Messages: If you recognize an email as spam or suspect it to be malicious, forward it to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). Let the company or person that was impersonated know about the phishing scheme and report it to the Federal Trade Commission at FTC.gov/Complaint.

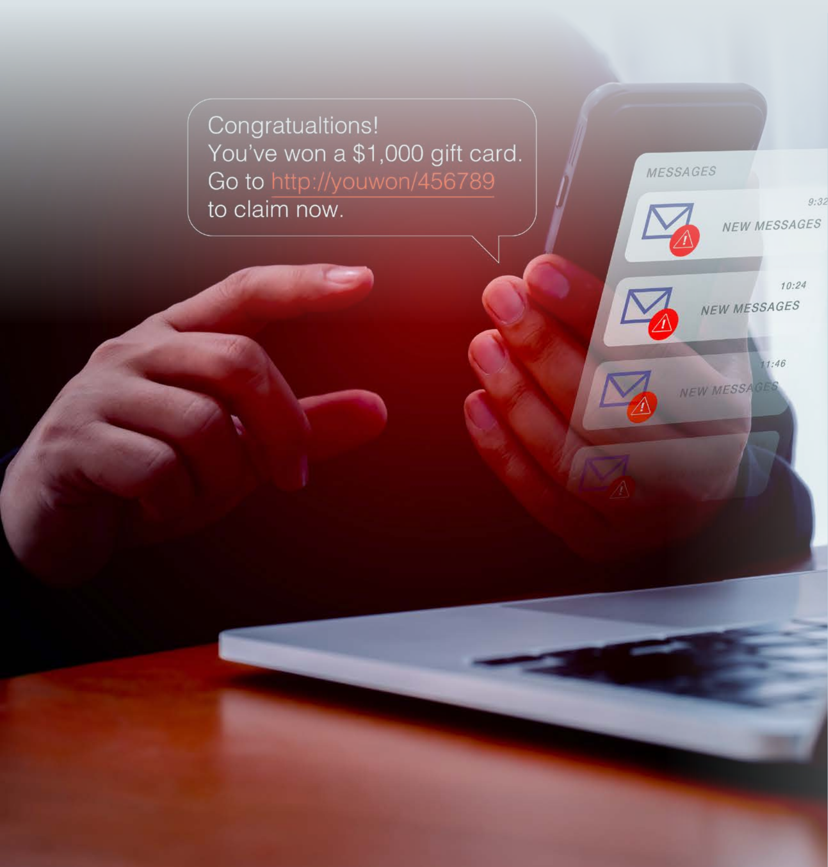


PRIZE SCAM

By FTC Staff

Scammers sometimes make you think you've hit a stroke of good luck. But if your million-dollar cash prize letter comes with instructions to pay a small fee — maybe for taxes, reporting, or handling — it's not luck. It's a scam. If you pay, you'll lose your money and find out there's no prize. Can you spot a prize scam?

Scammers use the promise of a prize to steal your money or your personal information. They might say they're from a well-known company like Publishers Clearing House and call, text, email, or message you on social media to say you're eligible for prize money. But they'll say you have to send them money first — maybe to pay a fee to release unclaimed money, for example. No real company will make you pay to claim a prize. Only a scammer will. Before responding, slow down and ask yourself these questions:



- **What do others say?** Search online and see what you find about the contest or company. Type the name with terms like "review," "complaint," or "scam."
- **Did anyone else get this message?** While you're checking online, see if others report getting the same message. If you got the offer by mail, look at the postmark on the envelope or postcard. A bulk rate means other people got the same offer.
- **Did they ask me to pay or give sensitive personal information?** If so, it's a scam. There's no reason to give your bank account or Social Security number to claim a prize. And only a scammer will insist you pay by wiring money through a company like Western Union or MoneyGram, using a payment app like Apple Pay, CashApp, PayPal, or Zelle, sending cash, or paying with gift cards or cryptocurrency to get your prize.

Share this alert with family and friends to help them avoid prize scams too. If you spot one, tell the FTC at ReportFraud.ftc.gov. Visit Prize and Grant Scams for more information.

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 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.