TruStage™

RISK Alert

Actionable insights for bond policyholders

Awareness | **Watch** | Warning

Fake auto dealers lure buyers with spoofed online ads

Law enforcement agencies across the nation have issued warnings about a new sophisticated fraud scheme that lures car buyers into sending money for a vehicle – sight unseen – to fake auto dealers. Fake auto dealers often use cloned websites or stolen photos to trick buyers into sending money for cars that don't exist. The scam involves creating a seemingly legitimate online presence with deals - too good to be true - in an attempt to steal funds or personal information.

Alert details

Law enforcement agencies across the nation have issued warnings about a new sophisticated fraud scheme that lures car buyers into sending money for a vehicle – sight unseen – to fake auto dealers.

One aspect of the trend involves fraudsters creating fake storefronts online. The scam starts when criminals create a website or social media profile claiming to be a legitimate dealership. After they create the website, they steal legitimate listings off other dealerships or create new ones using stock photos. As it turns out, the dealer cloned sites are just the bait that is used to get buyers to send irreversible wire transfers for cars they will never receive. The scam can be very convincing by featuring cars listed for sale on Carfax.com, Edmunds, and Facebook marketplace – but the fraudster creating the fake online ad does not actually own the vehicle.

For members considering an online vehicle purchase, watch for these red flags:

- Price seems too good to be true
- Limited or poor-quality photos
- Mismatched details, mistakes, and typos
- Refusal to allow physical inspection of the vehicle prior to purchase, rather insisting on delivery and demanding payment via wire transfer
- High-pressure sales tactics – there is another buyer seriously considering the vehicle
- Dealer refuses to provide their physical address
- Cloned or spoofed websites – scammers often create fake websites to mimic a legitimate dealer. The website URL may appear odd or incomplete with stock images and missing pages.

Date:
January 29, 2026

Risk category:
Consumer fraud; Loan fraud; Lending; Scams; Website spoofing

States:
All

Share with:

- Branch operations
- Executive management
- Loan Manager
- Loan staff
- Risk manager

Facing risk challenges?:
Schedule a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.

Risk mitigation

For credit unions working with members on vehicle purchases, consider providing members with the following risk mitigation recommendations:

- Encourage members to always physically inspect the vehicle prior to transferring payment. If it is not possible to personally inspect the vehicle, consider a trusted third-party like a local mechanic to represent the buyer.
- Research the seller/dealer. Confirm the dealer exists and that you are communicating directly with the legitimate dealer. Google the phone number in the ad (website) to see if there have been complaints or reports of fraud.
- Look up the address on Google Maps – does the image confirm an auto dealer lot?
- Avoid sending payment or deposit using a method that does not allow for recourse, (i.e., wire transfers, crypto, or gift cards). An escrow service can be used to ensure funds are not released until the vehicle is delivered.
- Always request the Vehicle Identification Number (VIN) and utilize an independent verification service to order a vehicle history report (i.e., Carfax or AutoCheck).

If a member believes they have been scammed, they should:

- Report the scam to the FTC at www.ReportFraud.ftc.gov
- Report to the State Attorney General's office or the Consumer Protection Division
- File a complaint with the Better Business Bureau

Risk prevention resources:

Access the **Business Protection Resource Center** for exclusive risk and compliance resources (user ID and password required).

Check out related resources :

- Don't fall victim: Consumer fraud & scams
- Member tips: Common consumer scams
- Protecting your identity & money
- Employee interactive training module: When members become victims

Access related RISK Alerts within the RISK Alerts Library. Simply use the search or other filtering features using keywords such as scams and fraud.

For additional support, call 800.637.2676 or email riskconsultant@trustage.com

TruStage™