



RRB News

U.S. Railroad Retirement Board

844 North Rush Street Chicago, Illinois 60611-1275

www.rrb.gov
877-772-5772 general information

Public Affairs
312-751-4777
opa@rrb.gov media inquiries

No. 26-6

For Immediate Release
September 2026

Railroad Retirement Board Urges Customers to be Wary of Scams

The U.S. Railroad Retirement Board (RRB) encourages railroad employees, retirees, and family members to be ever vigilant in avoiding fraudsters and scammers. The primary defenses against falling victim to this type of activity are caution and common sense.

The continued development of artificial intelligence (AI) can make it easier for bad actors to customize and personalize their schemes, which often involve impersonating a trusted entity, such as a family member or a government agency. AI can also be used to imitate dialogue and bypass spam filters, making it harder for people to distinguish between genuine and fraudulent communications.

These efforts often involve phishing emails, which try to entice recipients to surrender personal information, such as a social security number or bank account, or click on a malicious link. Another approach involves telephone calls in which the caller ID impersonates a local number or that of a bank or government agency.

The RRB typically sends official benefit-related communication to its customers via the U.S. Postal Service, with contact information specific to each notice. While the RRB may request certain personal information over the phone to verify the caller's identity, government agencies do not solicit personal information over the phone or by email or request advance fees or payment for services in the form of wire transfers or gift cards. This includes the RRB, as well as the Social Security Administration and the Internal Revenue Service.

In terms of emails, while the presence of typos or grammatical errors often indicates a fraudulent email, their absence is not proof of authenticity. If an unexpected email asks for personal or financial information, or directs the recipient to click on a link, it is best to avoid responding and to verify the request directly with the identified entity, either by email or phone. The same approach applies to telephone calls, particularly if you feel pressured, rushed, or threatened. **In such an instance, assume the call is fraudulent, hang up, and verify directly with the source.**

(More)

Scammers can also use AI to create fake social media accounts or web pages, often using government agency images, colors, and jargon, making it difficult to distinguish them from official ones. Warning signs can be social media accounts with a low number of followers, requests for payment for government forms or documents that are free, such as a replacement Medicare card, and links to websites that do not end in “.gov”.

If customers receive communication that causes a strong emotional response or a feeling of being pressured or rushed, they should pause, take a deep breath, and talk to someone they trust. They should hang up or ignore the message and delete it, without clicking on links or attachments. In addition, they are encouraged to be cautious of any contact claiming to be from a government agency or law enforcement telling them about a problem they do not recognize, even if the caller has some of the recipients’ personal information.

RRB customers unsure of the legitimacy of a phone call, email, website, or other communication should call the RRB toll-free at (877) 772-5772 for verification.

Other recommended actions are safeguarding personal information, including storage of an individual’s social security card in a secure location, shredding documents with personal information such as social security numbers, Medicare numbers, and financial accounts, and strong passwords for online accounts. Third-party software providing anti-virus protection, credit and identity monitoring, and password management can also provide added protection.

If a customer receives communication from someone impersonating the RRB or one of its employees, they should call the agency’s Office of Inspector General at (800) 772-4258 or send an email to **hotline@oig.rrb.gov**.

Other resources include the following websites:

- **www.identitytheft.gov**
- **www.consumer.ftc.gov/scams**
- **www.aging.senate.gov/scam**
- **www.medicare.gov/basics/reporting-medicare-fraud-and-abuse**