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. 20-2

For Immediate Release
February 2020

Railroad Retirement Board Reminds Customers to Avoid Scams

The U.S. Railroad Retirement Board (RRB) is reminding its customers to use caution and common sense to avoid being the victim of a telephone or email scam. Should there be some type of issue with an individual's account or benefits, the RRB will typically communicate with that person by sending a letter through the U.S. Postal Service. Such written notices contain contact information specific to each notice.

With the dramatic increase in "robocalls," in which automated dialing systems can disguise their source or even impersonate other numbers on caller ID, the opportunities for fraud and identity theft increase. The danger is not limited to the telephone, as scammers also use email as a means of obtaining personal information or money from unsuspecting recipients, often by impersonating a government agency.

While the RRB may request certain personal information over the phone to verify a person's identity, RRB employees will never use threats to obtain information or demand payment in exchange for some official action. Similarly, they will not ask for a credit card number or demand payment in the form of cash, money orders or gift cards. Asking for these types of payment is typical of a fraud, as these transactions are difficult to trace and often non-refundable.

If anyone pressures you to provide information or money over the phone, assume the call is fraudulent and hang up.

In addition to some of the previously described threats, emails often appear to be legitimate through use of seals or letterhead. And while misspellings or grammatical errors may indicate that an email is from a scammer, people should not assume that the lack of them makes an email legitimate.

(More)

There are steps that individuals can take to protect their personal information from fraud. These include the following:

- If you get an inquiry from someone saying they represent a company or a government agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request. (You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.)
- Store your social security card in a secure location, and avoid carrying it with you.
- Shred documents that list personal information, including social security numbers, Medicare numbers, and bank/credit card information.
- Maintain strong passwords for online accounts and use anti-virus software.
- Avoid opening emails, links or attachments from unknown sources.
- Promptly review any bank or investment account statements and notify the account manager of any unauthorized transactions as quickly as possible.
- If you answer the phone and the caller - or a recording - asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.

People should be particularly vigilant in the coming months, as scammers often impersonate employees of the Internal Revenue Service or state tax collection agencies during income tax season.

If you receive a suspicious phone call, simply hang up. Likewise, if you receive a questionable email, delete it without clicking on any links or opening attachments. If the caller or sender is impersonating an RRB employee, please report this behavior immediately to the RRB's Office of Inspector General by phone at (800) 772-4258 or email at ***hotline@oig.rrb.gov***.

# # #