UNITED STATES
POSTAL SERVICE

December xx, 2022

ALL EMPLOYEES

SUBJECT: Keep your private information secure

Maintaining the privacy of your personal data is a shared priority for you and the Postal Service. Your private information stored online is a target for criminals who seek to compromise this data for their financial gain.

Cyber criminals continue to be a threat by creating fake websites that closely resemble LiteBlue. These fake websites may feature an address ("URL") that is similar to the actual address, such as "LightBlue," "LiteBlu," or "LiteBlue.org", see the included handout ("Keeping Your Private Information Secure"). These fake websites may even forward you to the actual LiteBlue website once you enter your credentials. If you access one of the fake websites that closely resemble LiteBlue, cyber criminals can capture your employee identification number and password, which they can use to access your personal information housed within PostalEASE, including your direct deposit and other payroll information.

As an additional safety measure, the Postal Service has recently implemented a new email notification that will notify you of changes via your personal email address on file with the Postal Service. Instructions are in the included handout ("Updating Your Preferred Email Address"), outlining how you can access Employee Self-Service to update your personal contact information, including the email address and phone number that you have on file with the Postal Service.

Additional measures you can take to keep your account information safe:

- Do not share login credentials with others, including managers, co-workers, and outside entities.
- Keep your Employee Identification Number (EIN) confidential.
- Connect to USPS applications using secure connections that avoid public Wi-Fi or public computers.
- Any time you login to LiteBlue, check your account for any unusual activity.
- Save the LiteBlue website address (https://liteblue.usps.gov) as a favorite.

As a reminder, passwords are the first line of defense against potential cyber threats. You should always maintain strong, unique passwords for your online accounts. USPS passwords require:

- A minimum of 15 characters;
- Upper- and lower-case letters (A-Z) (a-z); and
- Numbers (0-9)

If you believe your account has been compromised, contact CyberSecurity Operations Center (CSOC) immediately, at CyberSafe@usps.gov.

Sincerely,

Jenny Utterback Vice President Organization Development	Heather Dyer Vice President Chief Information Security Officer

Encl. Handouts (Keeping Your Private Information Secure; Updating Your Preferred Email Address)