NATIONAL ASSOCIATION OF POSTAL SUPERVISORS
National Headquarters
1727 KING STREET, SUITE 400
ALEXANDRIA, VA 22314-2753
(703) 836-9660

January 26, 2023

Board Memo 004-2023: Multifactor Authentication for LiteBlue

Executive Board,

Cybercriminals pose a threat to postal employees by creating fake websites which resemble LiteBlue. In response to the issue addressed in Board Memo 043-2022, the Postal Service deployed the Multifactor authentication (MFA) tool on January 15. This tool is available to prevent cyberattacks and will provide additional protection for USPS employees and their personal information.

Attached is a draft of a home mailer, which will be sent out in the next few weeks to employees who still need to establish an MFA account. Also attached is an FAQ document.

Please share this information with your membership.

Thank you, and be safe.

NAPS Headquarters

UNITED STATES
POSTAL SERVICE

ALL EMPLOYEES

SUBJECT: Multifactor Authentication for LiteBlue

Cyber criminals continue to pose a threat to postal employees by creating fake websites that closely resemble LiteBlue. These bad actors leverage these fraudulent websites to capture employee identification numbers and passwords, which can be used to access personal information housed within PostalEASE, including direct deposit and other payroll information. These fake websites feature an address (“URL”) that resembles the actual address, such as “LightBlue,” “LiteBlu,” or “LiteBlue.org”.

Over the last few weeks, the Postal Service has taken steps to educate you of the threats that cyber criminals pose and what you can do to protect yourself along with technology changes to enhance our existing security protocols. These steps include a targeted awareness communication campaign to include a letter sent to all employees’ address of record and distribution of two required stand-up talks. We implemented email notifications to employees when changes have been made to their net-to-bank and allotment accounts and provided instructions to employees on how to set up this functionality.

Multifactor authentication (MFA) is an additional tool available to prevent cyberattacks and will provide additional protection for our employees and their personal information. MFA is a verification method requiring users to provide their username and password and an additional factor (authenticator app, one time passcode) prior to being allowed access to an application.

On Sunday, January 15, the organization deployed the MFA solution for LiteBlue as an additional security measure to protect employees’ IDs, passwords, and other personal data from unauthorized access and misuse. At this time, you are required to sign up for MFA to obtain access to LiteBlue. As a part of the MFA implementation, there are a few steps employees must complete. These steps include:

1. Reset your Self-Service Profile (SSP) password.
2. Verify answers to security questions.
3. Verify the last four digits of your Social Security Number (new security enhancement).
4. Establish MFA preferences.

As a part of our plans to mitigate the risk of continued attacks, transactions of net-to-bank and allotments were temporarily disabled for all employees; this functionality was re-activated on Friday, January 27.

It is important to note that your current net-to-bank and allotment settings remained the same with <u>no impact</u> to your established elections within PostalEASE. The temporary

disabling of net-to-bank and allotment transactions was only to prevent <u>new</u> transactions that <u>change</u> your current settings.

For information on setting up MFA or to view support materials, please visit the Multifactor Authentication page via the QR code below.

Jennifer D Utterback

Jennifer D. Utterback
Vice President
Organization Development

Heather L Dyer

Heather L. Dyer
Vice President
Chief Information Security Officer

Net-to-Bank and Allotment Transactions

Question: Is my paycheck affected by the temporary disablement of net-to-bank and allotment transactions?

Answer: Your current net-to-bank and allotment settings will remain the same with **no impact** to your previously established elections within PostalEASE. The temporary disabling of net-to-bank and allotment transactions was to prevent **new** transactions that **change** your current settings.

Question: When will net-to-bank and allotment changes in PostalEASE be re-activated?

Answer: With the successful implementation of MFA, the ability to make changes to your net-to-bank and allotment settings will be re-activated on Friday, January 27. At that time, you may access PostalEASE via LiteBlue utilizing your preferred MFA verification method.

Please note, in the interim, employees may cancel allotments, establish net-to-bank, or make changes via the **PostalEASE Interactive Voice Response (IVR) system**. IVR is a telephone-based system and may be accessed by calling the Human Resources Shared Service Center (HRSSC) at 877-477-3273, menu option 1. Employees using the IVR system will need to have their employee identification number (EIN) and personal identification number (PIN).

General Questions

Question: I am a contractor with the Postal Service, does MFA impact me?

Answer: No. Since your personal information is not housed on the LiteBlue postal network, you are not impacted by the SSP password reset or MFA requirements.

Question: Why is Multifactor Authentication (MFA) being required for LiteBlue?

Answer: MFA is a tool to assist the Postal Service in preventing cyberattacks and protecting you and your personal information. It provides an additional level of security to help protect your ID, passwords, and other personal data from unauthorized access and misuse.

Question: How do I set up my MFA preferences for LiteBlue?

Answer: Follow the step-by-step instructions in the User Guide and/or Videos posted on the MFA Blue and LiteBlue pages to establish your MFA preferences.

Question: Am I required to have a postal cell phone for MFA?

Answer: No, you can use any phone for MFA.

Resetting your SSP Password

Question: Why can't I sign in to LiteBlue?

Answer: After January 15, you will be unable to access LiteBlue until you reset your Self-Service Profile (SSP) password and establish your MFA preferences. Please refer to the User Guide and/or Videos posted on the MFA Blue and LiteBlue pages for further instructions.

Question: I am trying to reset my SSP password but do not know the answers to my security questions. What can I do?

Answer: The security questions related to your SSP password were established by you in a previous visit to LiteBlue. If you cannot recall your security responses, please select "Forgot Answers" and follow the prompts, including the selection of Email or First-Class Mail verification.

a. Email Verification
    1. Only select the email option if you have previously established a preferred email address within LiteBlue and you are able to access the account.
    2. Navigate to your email account and follow the prompts in the email.
    3. If you can no longer access the email account on file, do not recall the account, or have not previously established your email preferences, please select First-Class Mail as described below.
b. First-Class Mail Verification
    1. This method will provide further instructions via First-Class Mail at your address of record. Please allow 1 week for your letter to arrive. Once the letter is received, follow the prompts to continue resetting your SSP password.

Establishing your MFA Preferences

Question: What should I do if I do not have Google Authenticator or OKTA Verify on my smartphone?

Answer: To utilize these MFA preferences, you must download the application from your smartphone's App Store. Please refer to the User Guide and/or Videos posted on the MFA Blue and LiteBlue pages for instructions on how to download these options. Alternatively, you can select the "Phone" MFA option, which does not require a smartphone.

Question: What if I do not have a smartphone?

Answer: If you do not have a smartphone, you can select the "Phone (Voice)" MFA option and utilize any phone to include a landline. This MFA method allows you to proceed without the use of a smartphone by receiving your verification code via a voice message in the form of a phone call. Additionally, if your phone receives text messages, you may select the "Phone (SMS)" MFA option as well.

Question: If I am using a postal smartphone, where do I find the Google Authenticator or OKTA Verify applications?

Answer: If you are utilizing a postal smartphone, OKTA Verify and/or Google Authenticator can be found on the USPS AppStore on those devices. You may utilize the search feature to locate both applications.

Question: When setting up Google Authenticator or OKTA Verify on my smartphone, how do I scan the QR code?

Answer: When establishing OKTA Verify or Google Authenticator you must select “OK” when your phone notifies you that “OKTA Verify” or “Google Authenticator” would like to access the camera. Enabling this feature within the application will automatically enable you to point the camera on your phone at the QR code and scan it.

Question: Does it matter what type of smartphone I have? (iOS, Android)

Answer: No, you can use either an iPhone (iOS) or Android model smartphone. Please note: The screenshots in the User Guide and Videos are from an iOS device. If you are utilizing an Android smartphone, your screen may appear slightly different. However, the steps for authentication remain the same.