DATE

Individual Name

Address/work and home

Redemption Code:

I am writing to inform you that the United States Postal Service's (Postal Service) Corporate Information Security Office (CISO) detected unusual log-in activity involving a limited number of employees' accounts within the Postal Service's PostalEASE system, including your account. Upon further investigation, it appears that your login credentials have been compromised. As a safety measure, your PostalEASE account has been auto locked and you will be required to reset your password and change your challenge questions and answers.

PostalEASE is a self-service web application that is your gateway to many postal employment-related services, including LiteBlue. The PostalEASE application has not been compromised; it remains secure. However, as noted, it appears that your login credentials have been compromised.

We believe your login credentials were compromised when you interacted with a fake LiteBlue website. We are unable to determine if this interaction was recent or whether it occurred sometime in the past.

The United States Postal Inspection Service, Office of Inspector General, and CISO discovered fake LiteBlue websites that accurately mimic the actual LiteBlue website. The official LiteBlue website is https://liteblue.usps.gov.

These fake websites may feature an address ("URL") that is similar to the actual address, such as "LightBlue," "LiteBlu," or "LiteBlue.org." Scammers use these fake websites to collect employee login credentials. Once employees attempt to log in to the fake LiteBlue site using their credentials, the scammer records the information, which they can then use later to enter PostalEASE and access the employee's sensitive information. This information may be leveraged by the scammer or others for identity theft or other criminal purposes.

The Postal Service continues to take precautionary measures, including identifying and notifying potential victims; reviewing suspicious account activity; resetting credentials; and working with internet service providers to identify fake websites. We plan to continue investigating and monitoring the PostalEASE application on our network to mitigate the risk of unauthorized activity.

The Postal Service will purchase a 1-year credit monitoring service on your behalf due to the sensitive nature of the information about employees that is accessible through PostalEASE. Enclosed with this letter, you will find information on how to enroll in the credit monitoring service for 1-year at no cost to you. Please note the redemption code provided at the top of this letter, which will be required when you contact the credit monitoring company. You have 90 days from the date of this letter to take advantage of the credit monitoring service. We encourage you to take advantage of this service.

In addition to the Postal Service's ongoing monitoring efforts and the offered credit monitoring service, you will be required to reset your PostalEASE password and change the challenge questions and responses in PostalEASE.

To reset your password, go to liteblue.usps.gov and select "Forgot my Password." This will take you to the employee Self-Serve Password tool, where you will change your password and security

questions. Once reset, your password and new security questions will be available immediately. Please log in and verify your ability to access your PostalEASE account after you change your password and security questions.

You can increase the security of your account by selecting a new, unique password. We recommend making passwords unpredictable; avoid using names, including pets' names, dates, or often-used words that can be discovered. You should **never share your password** with anyone, including individuals or other third parties who request your EIN and password to provide financial or other services.

If you are interested in other resources that can be used to protect your identity, the Federal Trade Commission (FTC) is a good source of information. The FTC's website (www.ftc.gov) provides helpful information regarding identity theft and data protection. You can find information on identity theft from the FTC at https://www.consumer.ftc.gov/features/feature-0014-identity-theft, or you may call the FTC's Identity Theft Data Clearinghouse at 1-877-438-4338 (TTY: 1-866-653-4261). In addition, you may also request a free credit report online at www.annualcreditreport.com.

Here are some additional resources to assist you going forward:

To report fake USPS websites, please email cybersafe@usps.gov

Should you identify any activity with your account that looks suspicious in the future, contact ISCCU@usps.gov

For PostalEASE account issues, contact the Human Resources Shared Services Center at 1-877-477-3273.

Please direct any questions regarding direct deposits or allotments to the Accounting Help Desk at 1-866-974-2733 and identify yourself as an active employee.