UPDATES: POSTALEASE / E-OPF / UNIFORM & WORK CLOTHES ANNUAL ALLOWANCE CARRY OVER

Teresa Harmon, Manager, CAD

In this month's article, I want to give you some updates on various issues.

PostalEASE

Here is an update on the status of the national grievance that was filed on the fraudulent access on PostalEASE. To give some background on this case, on December 20, 2022, the Union received notification from the Postal Service that the Postal Service had confirmed that some employees had unknowingly provided their usernames and passwords to criminal websites while attempting to access PostalEASE. We were told that employees had used Google to access PostalEASE and that Google in turn was redirecting them to third party criminally-run websites that mirrored the look and access of PostalEASE. This resulted in the login credentials being hacked and accounts compromised. With access to login credentials, the criminals were able to go to the official PostalEASE site and add allotments that were then deducted from the employees' checks. These added allotments were sent to various bank accounts which were set up by the criminals allowing them to withdraw all the funds. The Postal Service informed us that they would not be providing any monetary reimbursements where the employees accessed the criminally-run websites and had their credentials hacked.

Earlier last year we also submitted an official information request regarding this fraudulent activity to obtain additional information to better understand what happened, who was responsible, and the Mail Handlers that were impacted and how much of their pay was lost. The Postal Service refused to provide us with certain information that was requested. We had to file a NLRB charge to try to obtain this information. As a result of the NLRB charge, the Postal Service agreed to provide much of the information we were requesting, including that they agree to send a letter to our affected members to provide them with the option of contacting us directly or submitting a privacy waiver to the Postal Service to authorize the Postal Service to release their information to us. These letters were sent out to the affected mail handlers on July 14, 2023.

Earlier last year we also submitted an official information request regarding this fraudulent activity to obtain additional information to better understand what happened, who was responsible, and the Mail Handlers that were impacted and how much of their pay was lost.

The NPMHU filed a national-level grievance on February 16, 2023, over the failure of the Postal Service to pay these individuals. After much discussion, the Postal Service denied the grievance, and the case was appealed to arbitration.

The NALC and APWU also filed national disputes on this same issue. The NALC case was the first to be scheduled for arbitration. Their arbitration hearing took place in front of Arbitrator Dennis R. Nolan on Jan. 23–24, 2024, in Washington, DC. Both the APWU and the NPMHU intervened in this hearing, siding with the NALC. It is the position of all three Unions that the Postal Service failed, among other things, to take even basic steps to secure the PostalEASE site, such as implementing multi-factor authentication (a security measure that is common with most online financial transactions). As a result, the Postal Service has an obligation to compensate these employees for their work and to make them whole. The Postal Service's failure to pay these individuals violates numerous provisions of the National Agreement. Management has the responsibility to safeguard its employees from this type of criminal activity by ensuring that USPS-controlled websites are secure. An update will be provided once the

arbitrator renders his decision, which could take several months.

eOPF

eOPF has been shut down since December 15, 2022, due to the Vice President, Chief Information Security Officer becoming aware of a security issue involving full social security numbers being displayed on some of the documents that are part of employees OPFs. The Postal Service has had problems finding software that would be able to mask all the different types of documents that are part of the OPF. They have now purchased a data tool that can perform those functions and are anticipating that eOPF will be reactivated by the end of May 2024.

UNIFORM AND WORK CLOTHES ANNUAL ALLOWANCE CARRY OVER

Effective March 13, 2024, the following provision of Article 26, Section 26.3 of the 2022 National Agreement will be implemented:

> Unused portions of an eligible employee's annual allowance for uniform and work clothing will be carried over and available for use beginning twelve (12) months after the end of each anniversary year. An eligible employee's uniform and work clothing allowance balance may not exceed the sum of two (2) years of the employee's annual allowance entitlement. This uniform and work clothing program adjustment will be implemented no later than twelve (12) months from the ratification date of the 2022 Agreement.

Starting March 13, 2024, any unused portion of an eligible employee's annual allowance will be accumulated and will be reflected in the employee's uniform allowance accounts starting March 13, 2025 at the end of each employee's anniversary year.

AFTER JANUARY 15, 2023 USPS EMPLOYEES ARE REQUIRED TO SET UP MULTIFACTOR AUTHENTICATION (MFA) TO ACCESS LITEBLUE.

MULTIFACTOR AUTHENTICATION (MFA) REQUIRES A PERSON TO PRESENT (2) DISTINCT 'FACTORS' WHEN ATTEMPTING TO REGISTER FOR LITEBLUE. USPS.GOV.

WHAT ARE AUTHENTICATION FACTORS?

- Something you know (e.g. password, passphrase, PIN)
- Something you have (e.g. phone, ID Card, key fob)
- Something you are (e.g. biometrics, keystroke patterns)

BENEFITS OF MFA

- Increases assurance that only the user (you) will be able to access an account, application or device.
- Reduces impact of credential theft (stolen password or username)

COMMON MFA METHODS

- Use of a One-Time password
- Approve a Push Notification
- Receive a code via phone call.
- Receive a code via SMS/text message.