Payment Redirect Fraud Risk Mitigation

As the bank for Washington and its state agencies, the Office of the State Treasurer (OST) Acts upon your payment instructions for payroll. Since OST must act upon your payment instructions, agencies are responsible to confirm the validity of employee banking information prior to updating HRMS. Payment Redirect Fraud occurs when a fraudster, who is impersonating the legitimate recipient of a state ACH payment (such as employee pay or travel reimbursement), updates the banking information, redirecting the payment to an account the fraudster controls. State and local governmental agencies face potential losses from this type of fraud.

OST would like you to be aware that Payroll is often the target of this scheme. Following these industry best practices will help mitigate risk.

- Send employee account change confirmation letters. Run the job in the HRMS to generate a confirmation letter when bank details have been updated.
- If the employee didn't deliver the form in person, call or email to confirm the employee submitted a request. Fraudsters will often email, fax, or mail change request forms. Use phone numbers or email addresses from state agency address books to contact the employee. Do not reply - start a new email chain if the form was received by email.
- Do not make account changes based solely on requests received over the phone or email. Require a completed Authorization for ACH Direct Deposit form.

Please feel free to reach out to Lesa.Williams@tre.wa.gov with any related questions.

Last updated January 16, 2024