Payment Redirect Fraud Risk Mitigation

An increase in agencies victimized by Payment Redirect Fraud has been reported to the Treasurer. 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. Several state and local governmental agencies have incurred losses from this type of fraud.

OST would like you to be aware that Payroll is often the target of this scheme. While no procedure will prevent fraud 100% of the time, following these industry best practices will help mitigate risk.

- Send employee account change confirmation letters. Run job in HRMS to generate a confirmation letter when bank details have been updated.
- If the employee didn't deliver the form in person, call/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 book to contact the employee. Do not reply - start a new email chain if the form was received by email.
- Do not make account changes requested over the phone or email. Require a completed Authorization for ACH Direct Deposit form.

Last updated October 2, 2020