PAYSERV
PAYROLL SOLUTIONS

How do I Protect My Company and My Employees from Direct Deposit Fraud

- **Employee Self Service (ESS)**
  Sign up for ESS and require employees to log into www.payserv.myisolved.com to update their direct deposit information themselves. This is a secure website with multi-factor authentication to ensure that employees really are who they say they are and eliminates the middleman when employees are updating their account information. Workflows can be set up that allow you to receive notification that your employee made the request allowing you to make the approval or denial choice in the system. Step-by-step instructions on how to set up ESS, change direct deposit information or set up a workflow are available. Please contact you Payroll Specialist for assistance.

- **Direct Deposit Changes**
  Do not accept direct deposit changes from employees via email! It is easy for spoofers to create a fake Gmail account or hack an employee's email account and pretend to be the employee. Always verify with the employee in person or by phone that they actually want to change their direct deposit information and that the information being submitted to payroll is accurate.

- **Direct Deposit Forms**
  If a client insists on submitting a direct deposit change on paper, we will only accept direct deposit change requests from our primary point of contact at your company, or specified designee. Our Employee Authorization for Direct Deposit form must be signed by the employee AND company contact indicating that the client has reviewed and approved the change request with the employee prior to submission. Unsigned direct deposit forms are not accepted or processed. Once the form has been received, our team will place a phone call to the client to ensure that the change has been authorized. Direct Deposit authorization request forms can be found on our website or through a link on your PayServ/isolved account landing page.

- **Require a voided check or bank direct deposit statement**
  A voided check or letter from the employees' bank to verify that routing and account information is correct. Direct deposit funds sent to the incorrect account cannot always be recovered once they are sent.

- **Strong Passwords**
  Ensure that your employees are using strong passwords for online applications, including their personal and work email accounts. Always use multi-factor authentication for personal and business email accounts. Fraudsters have also been known to hack email accounts and request changes from the employee's legitimate email account.

- **Pay Cards**
  If employees are using a pay card or if the banking looks suspicious, always triple check that it is the employee submitting the change and that the account information is correct. Pay cards are notorious for fraud and funds can almost never be recovered if sent to the incorrect account.

- **ID Theft Protection**
  Enroll your employees in Ultimate ID Plus through PayServ Perks to provide them with the #1 Identity Theft protection provider for consumers. This service delivers the most comprehensive identity theft solution that monitors, alerts, controls, protects and recovers! Contact your sales or payroll specialist for more details.