INTEGRITY
BOOKKEEPING • PAYROLL

Direct Deposit Fraud

EMAIL SCAMS

My employee sent me an email asking to change his/her direct deposit -- ARE YOU SURE IT WAS FROM YOUR EMPLOYEE?

Be aware that fraudulent emails are being sent posing as employees asking to change their direct deposit information. They will respond to emails and even send what appears to be a voided check for a new account. How do I know if the information is legit?

CALL YOUR EMPLOYEE to confirm. Make sure to confirm ANY direct deposit changes and/or ACH payment requests by PHONE.

This could apply to vendor payments as well as Employees so be on alert for any emails that come from one department to another within your organization. Always confirm by phone any requested ACH payment or change to banking information.

Once an ACH is sent through your bank, the ACH cannot be stopped.
For payroll, we are also limited on ACH reversals.
Diligence up front can potentially eliminate fraudulent losses.

What Should I Be Looking Out For??

RED FLAGS

1. Email address is not exactly right
2. Unusual for email/vendor to make request by email
3. Voided Check is not a scan but a generic form with employee name
4. Employee name may not be full name (or full name not usual nick name)
5. Signature looks off or is rudementary

6. New account is a pre-paid debit card or not a commonly used large bank such as Metabank, Sutton Bank, TD Bank, GreenDot, etc.

What Should My Employees Do?

REVIEW YOUR PAYSTUBS

It is surprising how many people never review their paystubs. Yes, paystubs are only generated **after** the payroll has been processed but any other problems with deductions, withholdings or account numbers can be seen then.

Have your employees setup their Employee Self-Service Portal (ESS)? If not, they can be accessed through this link. If you need your company code or setup instructions, please contact our offices for more details.

NEED HELP? Contact us for assistance.

IntegrityPAY
INTEGRITY BOOKKEEPING, LLC
payroll@integritypay.biz
614-591-4521