FRAUD PREVENTION AND AWARENESS

As ACH and Wire fraud continues to affect businesses in our area, we want to take a moment to stress the importance of verifying all invoice and account information changes. Once an ACH payment or Wire payment reaches the fraudsters account, the funds are immediately withdrawn and are not able to be recovered.

To avoid a monetary loss to your business, it's critical that procedures are put in place to verify any changes verbally with a known contact and not the contact on the invoice or the sender of the request if received via email. *It's also vital that employees are properly trained to follow the below procedures.* Education is the key to prevention.

For any email requests for payment or account information changes, implement STOP. CALL. CONFIRM.

- STOP – Do not process the request received via email.
- CALL – Call the "sender" using a legitimate phone number known to you. DO NOT reply to the email and DO NOT call the number listed in the email.
- CONFIRM – Verify that the real vendor or employee did, in fact, request the change.

COMMON TYPES OF ACH AND WIRE FRAUD

Vendor Impersonation Fraud occurs when a business receives a request, allegedly from a contractor that the business has previously paid, to update the payment information for that contractor. They could request an update to the routing and account information, or request that the payment method be updated from check to ACH. Without verifying this information with a known contact, the business could inadvertently send funds to a fraudster.

Business Email Compromise gives a scammer access to previous payment details which the scammer then uses to manipulate an employee into sending money. The scammer will pose as an executive at the company or even a known vendor and send an urgent email to an employee providing account information and requesting that funds be sent immediately. Often times, when it appears the email is coming from the CEO, the employee will complete the payment without question.

Payroll Fraud happens when a fraudster sends an email to someone in your HR department, or payroll clerk, that is designed to look like it's coming from an employee. The email is requesting a change in the employee's direct deposit account information. If the scam is successful, the money is diverted to the fraudsters bank account. In another version of the scam, the fraudster will send a phishing email directly to the employee, designed to appear as if it's coming from their employer, to get that employee to divulge information that will allow the scammer to access his or her payroll information.