CYBERSECURITY ALERT

PROTECTING THOSE WE SERVE

VALIDATE ALL CHANGES TO PAYMENT INSTRUCTIONS

ALERT:

Criminals have been targeting companies by posing as vendors and changing payment instructions so money is sent to fraudulent bank accounts. In these instances, criminals are using masked email addresses, false domain names and/or compromised email to execute the schemes.

In all cases, recipients did not contact their vendors to confirm the new banking instructions before releasing the funds.

What you can do.

SOLUTION:

- Regularly check your accounts for unusual or suspicious transactions.
- Enable your online banking accounts to notify you of account changes and transactions.
- Validate all payment requests and invoices—even if they appear to be internal—either in person or by telephone to an authorized representative using a known contact number. This includes any changes to vendor payment information, such as banks or account numbers.

The information provided here is intended to help customers protect themselves from cyberfraud. It does not provide a comprehensive list of all types of cyberfraud activities or identify all types of cybersecurity best practices. Your company or organization is responsible for determining how to best protect against cyberfraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs.

Remember, there is an increased risk of fraud losses if you don't use the appropriate fraud-prevention tools. You are liable for payments originated with your authorized users' security credentials or by other people with transaction authority.