Citizens Commercial Banking®

Helping you protect your business from fraud

Dear Valued Client:

In support of our efforts to protect your personal information from fraud and identity theft, we wanted to make you aware of an increase in fraudulent activity using a known industry threat called Business Email Compromise (BEC). BEC occurs when fraudsters send emails that impersonate a CEO (or other senior executive within the company) or a known vendor of that company.

No bank systems have been compromised, but protecting your business from fraud and keeping you aware of cyber-security measures is extremely important to us. In cases of fraudulent activity, we will attempt to recover any funds on behalf of our clients.

How the scheme works
In one scheme, fraudsters send fraudulent instructions, often claiming to be urgent, via email from what appears to be a high-ranking company official to account administrators with wire/transaction authority and/or capability within the company. The recipients often act upon the enclosed instructions, as the emails appear to be legitimate requests from authorized company personnel.

Another scheme involves a company receiving an email (or a phone call), supposedly from a vendor, advising that the vendor's payment information has changed. Later, when the actual vendor requests payment, the company initiates the wire – with payment going to the fraudster.

Suggested Controls and Preventative Measures
As your trusted advisor, we want to share the following practical controls that can help combat those schemes:

1. Remember that even an email sent from what appears to be a familiar

address may be fraudulent. Remind employees to look for subtle differences in the email address.

Tip: Look for slight variations; for example, **firstname.lastname@company.com** may be spoofed as **firstname.lastname@*cornpany*.com**.

2. Do not automatically trust any email, phone call or letter from an unknown individual or organization.
3. Never open an attachment from an unsolicited email. Most importantly, never click on a link sent to you in an unsolicited email.
4. Confirm any request to change payment instructions by contacting a colleague or vendor by phone using a previously known valid number. Never reply to the email to confirm the instructions or ask clarifying questions.

To learn more, visit citizensbank.com/security or contact your Treasury Solutions Sales Specialist or Client Services at 877.550.5933 (Monday to Friday, 7 a.m. – 7 p.m. ET).

Your relationship is our highest priority and nothing matters more to us than your complete satisfaction and trust. Thank you for choosing Citizens Commercial Banking.