Citizens State Bank

Avoid imposter fraud. Impostor fraud involves a fraudster posing as a person or entity you may know and trust — an executive of your company, a vendor, even the IRS. The impostor contacts you by phone, email, or mail and submits an invoice or requests a payment or a change to vendor payment instructions. If you fall for the scam, any payments you send go to the fraudster instead of where you intended.

Guidelines for a strong fraud protection program

Here are some best practices you can use to help protect your accounts from online fraud.

- **Verify your vendors account number changes** – Require all changes to vendor payment account numbers to be made in writing on the vendor's letterhead and verified with a call to the vendor's telephone number in your files. You should always "Verify before you initiate" and "Verify before you approve."
- **Educate your employees** – Remind your employees not to click on links purporting to be antivirus or anti-malware software, do not download files from unknown sources or respond to ony screen pops; especially ones asking you to enter your contact information. Ignore pop-ups seeking your online banking credentials and be cautious of unexpected token prompts or unsolicited calls to assist you for unreported log-in issues.
- **Protect your access credentials** – Never give out your password, PIN or the PIN + token code combination. If you receive an email, phone call, or text message claiming to be from your financial institution, asking for this information, it is likely a **"phishing**" attempt. Do not respond to it. Report it to your financial institution immediately.
- **Strengthen your internal controls** – Implement dual custody on all online payment services (ACH, wire transfer, foreign exchange) and Administration services. Update antivirus and antispyware software and firewalls regularly.

To report fraud, immediately contact your relationship manager.