Protect Your Business

Best Practices to Help Protect Your Company from Fraud

- Conduct daily banking reconciliations
- Initiate ACH and Wire transfer payments under dual control and multifactor authentication
- Immediately escalate any suspicious transactions to Third Coast Bank SSB
- Install virus\malware\ransomware protection on all computer systems and ensure they are updated regularly
- Computers and servers should be patched regularly
- Consider spyware detection programs
- Verify use of a secure session (https, not http) in the browser for all online banking sites
- Avoid using automatic log-in features that save usernames and passwords for online banking
- Never leave a computer unattended while using any online banking service
- For businesses that conduct online transactions, it is recommended that commercial online banking activities be carried out from a stand-alone, hardened and completely locked down computer from which e-mail and web browsing are not possible
- Install a dedicated firewall
- Make frequent backups of your data
- Be suspicious of all emails, especially e-mails requesting account verification or banking access credentials such as usernames, passwords, PINs and similar information. Opening file attachments or clicking on web links in suspicious emails could expose your computers and systems to malicious code that could hijack your computers and your systems
- Create a strong password with at least 8 characters that includes a combination of mixed case letters, numbers and special characters
- Use a different password for each website that is accessed
- Only connect to WIFI networks that you absolutely trust. Turn off the automatic connect function on your mobile device.