

# PARAGON COMMERCIAL BANK

November 30, 2009

## An Important Message to All Paragon Clients:

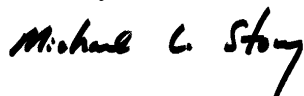
Within the last year, there has been a significant increase in online banking fraud involving small and medium sized companies, non profits, and public institutions. Paragon clients have been recently impacted by this fraud. A typical fraud scenario involves “phishing”, an email that looks legitimate (such as a bogus Microsoft Critical Update) but contains an infectious content sent to an employee of your company. Once the user opens an email attachment, or navigates to the referenced web site, malware is installed on the user’s computer. The malware will compromise the user’s online banking credentials and uses them to initiate fraudulent financial transactions such as wire transfers and ACH transactions. As of October 2009, there has been approximately \$100 million in attempted fraudulent transfers nationwide, and the threat is continuing to increase.

One of the most effective methods to protect yourself and your business is to establish a dual control environment for your wire and ACH transfers. We strongly recommend adding this additional level of security, as it is the most effective control to prevent internal and external fraud.

For your convenience, we have included some additional computing security recommendations with this letter. These will help improve your company’s information security.

We value our relationship with you and it is our hope that this information will help you protect yourself and your company from becoming a victim of fraud. If you have questions or concerns, please call me at 919-534-7444 or Jennifer Terry, our Chief Deposit Officer, at 919-534-7430.

Sincerely,



Michael L. Story  
Executive Vice President  
Chief Operating Officer

## ***Computing Security Recommendations***

### ***General Business Practices***

1. Review this letter with your IT department or consultant and evaluate how your systems may be vulnerable to this risk. Follow their advice to protect your system or individual computer from being used to perpetrate a fraudulent transaction.
2. Talk to your insurance provider about adding a cyber insurance rider to your business insurance policy.

### ***Passwords Practices***

3. Change passwords at least every 90 days and every time an employee leaves the company.
4. Ensure that the account information and security responses are not written down. If the information must be written down, it should be secured under lock and key when not being used.
5. Never share your user ID or password with anyone for any reason. If it is compromised, call and have the ID and/or password disabled or reset.
6. Secure your computers with a password protected screensaver with a 15 minute timeout.

### ***Operating System Protection***

7. Ensure that you use current anti-virus and anti-spyware products to protect yourself against malicious software that is created for the specific purpose of gathering information such as user ID, password, and other critical information that may be stored on your computer.
8. Ensure that you have a patch management solution that keeps your computer software current and can further mitigate new vulnerabilities to which your computer may have been exposed.
9. Practice safe internet use. Never click on pop up messages or links to applications. Try to get into the habit of manually going to links that are sent to you.
10. Use caution when opening attachments and ensure they were sent from a trusted source.
11. Consider designating a “locked down” PC to accommodate only your online banking transactions. This computer should not be used for email or any other internet activities. This precaution will minimize the opportunity to download malware.