



May 7, 2010

An Important Message to All Paragon Online Banking Clients:

Within the last year, there has been a significant increase nationally in online banking fraud involving small and medium sized companies, non profits, and public institutions. Unfortunately, certain Paragon clients have been 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 computer virus 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 use them to initiate fraudulent financial transactions such as wire transfers and ACH transactions. Attempted fraudulent transfers nationwide total more than \$100 million, and the threat continues 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 appears to be the most effective control to prevent internal and external fraud. Additionally, we suggest that you establish individual authority limits that are appropriate for the type of transaction performed.

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

We value our relationship with you and it is our hope that the enclosed 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,

A handwritten signature in black ink that reads "Michael L. Story". The signature is written in a cursive, slightly slanted style.

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.
3. Reconcile your banking transactions daily and look for unusual small amounts such as penny transactions. This may be an indication that your account has been compromised and a fraudulent plan is in progress.
4. Never access bank, brokerage or other financial services information at internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account numbers and sign on information leaving you vulnerable to fraud.
5. Immediately escalate knowledge of any suspicious transaction to the Bank, particularly if these transactions are ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent or minimize further loss.

Password Practices

6. Change passwords at least every 90 days and every time an employee leaves the company.
7. Create a strong password with at least 10 characters that includes a combination of mixed case letters, numbers and special characters.
8. Ensure that your account information and security responses are not written where they can be seen or accessed by others. If the information must be written down, it should be secured under lock and key when not being used.
9. Never share your user ID or password with anyone for any reason. If it is compromised, contact us to have the ID and/or password disabled or reset.
10. Secure your computers with a password protected screensaver that has a timeout feature activated after no more than 15 minutes.
11. Avoid using an automatic login feature that saves usernames and passwords for online banking.

Operating System Protection

12. 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.
13. 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.

14. Install a dedicated, actively managed firewall, especially if you have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and to computers.
15. Practice safe internet use. Never click on pop up messages or links to applications contained in emails. Try to get into the habit of manually going to links that are sent to you.
16. Be suspicious of emails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes and similar information.
17. Use caution when opening attachments and ensure they were sent from a trusted source.
18. 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 should minimize the opportunity to download malware.