Business Banking System Risk Controls and Best Practices

General

- ✓ Consider a dedicated computer for online banking that is never used for e-mail or general internet browsing. Install anti-virus, anti-malware, and anti-spyware and keep all security software updated. If you allow any outside vendors to access your company network, ensure they are implementing the proper security controls.

- ✓ Monitor account activity **daily** for anomalies or suspicious transactions and report to Navigant's security officer immediately at 401-233-4700 for further investigation. Keep access to Business Banking restricted to only those that need to have access.

- ✓ Verify the use of a secure session. (https:// vs http://)Upon login, when requesting your "one-time" login security code, choose the "out of band" voice or text message delivery option.

- ✓ Do not use the same User ID or password on any other website. Periodically change your passwords and avoid saving passwords to your computer. Never share your credentials with anyone and never access your business accounts through an unsecure wi-fi connection.

- ✓ Utilize email balance and activity alerts to monitor account activity.

- ✓ Immediately delete the user profile for any employee that leaves the company.

- ✓ Educate employees on good cyber security practices to avoid becoming a victim of fraud.

Money Movement

- ✓ The company administrator can issue ACH & Wire daily operation limits to employees who have permissions to move funds via Business Banking.

- ✓ Have a second person at the business approve submitted wire transfers and ACH files. The second person should use a different computer than the one used to initiate an action.

- ✓ Do not suppress any email notifications within Business Banking. They notify you of profile security changes and ACH & Wire payment activity for your protection.

- ✓ Never conduct business through email only. Be cautious of any email requesting you to change a beneficiary account number that you have been sending funds to all along. Follow up with a phone call to ensure the change is valid!

- ✓ Periodically prepare a company risk assessment to evaluate internal controls regarding conducting business online. Staying on top of the latest threats is key to protecting your business!

If you have any questions regarding the business banking system controls or implementing them for your company, please contact the Electronic Services department at 401-233-4700.