Business Online Banking Best Practices

Business Online Banking Tools
Add a stronger level of security within Business Online Banking by utilizing the following features:

Alerts:
- The alert functionality will send an e-mail to inform you when transactions are sent, when information is changed or when a transaction is waiting for approval.
- This will alert you very quickly to a potentially unauthorized transaction, and can be sent to two different e-mail addresses for additional protection.

User Access and Limits:
- The Admin tool allows you to set individual IDs to create an audit trail of activities by user. It also allows you to limit individual access to fit different employees' responsibilities.
- Do not use or share the Admin user ID for daily processing. This prevents the ability to create an audit trail.

Dollar Limits:
- Set up appropriate dollar limits by individual user.

Dual Control (Multiple Approvers):
- Set up multiple approvals on transactions that move money in and out of the bank.

Secure Tokens:
- The token is a physical device that generates a new six-digit code every thirty seconds. To log in, a user enters the six-digit code from the token device and the user PIN, both of which confirm the user's identity.
- Secure tokens are required for all customers originating ACH items or sending wire transfers online.

Out-of-Band Authentication:
- The system verifies user at login by taking into consideration usual customer behavior. If behavior varies, a phone call is initiated to a phone number on file. Login will not proceed until identity has been verified.

Business Online Banking Best Practices
It is important that all employees follow these security practices on a day-to-day basis:

Login:
- Before entering your password, ensure that the website you are visiting belongs to Park Bank. You are also advised to check that the website's digital certificate is issued to Park Bank.
- Ensure your session is encrypted. The website address should precede with https:// and a security icon that looks like a lock or key should appear near it.

Tokens:
- Safeguard your token and password at all times and don't allow anyone to keep, use or tamper with it.
- Do not reveal the one-time password generated by your secure token to anyone.
- Do not divulge the serial number of your secure token to anyone.
- Do not allow employees to share tokens. This increases your risk to fraud exposure.

Logoff:
- Log off from your online session when you leave the computer unattended and turn off your computer when not in use.
- Clear your Web browser cache and history after logging out. Close your Web browser to ensure that all your account information is removed.

User ID and Password Guidelines:

- Create a "strong" password with at least 8 characters that includes a combination of mixed case letters, numbers and special characters. Change your password frequently.
- Never share login credentials (user name, password, token number and pin) with third party providers.
- Do not store passwords on the same device used to access online banking.

Internet Controls & Recommendations:

- Never access bank, brokerage or other financial services information at cafés, airports, hotels, public libraries or any other networks that you do not control.
- Never respond to a suspicious email or click on any hyperlink embedded in an email from an unkown or suspect sender. For example, the Fed will never contact you directly if an ACH or wire fails.
- Educate your staff about current scams and loss-prevention steps.
- Use a unique password for each website that you access.
- Verify use of a secure session (https vs. http) in the browser for all online banking or financial web use.
- Never conduct banking transactions while multiple browsers are open on your computer.
- Limit access to social networking and personal email sites for employees.

System Controls & Recommendations:

- Conduct all online banking activities from a dedicated computer. Do not allow access to any email or websites other than the online banking site.
- Remove administrative rights on user's workstations to help prevent inadvertent installation of malware or viruses.
- Install anti-virus and desktop firewall software on all computer systems. Update regularly and if updates no longer available, your operating system may need to be updated.