Is your Business Protected?

Fraud is one of the largest threats facing businesses today. Unfortunately, most businesses don't take proper precautions until a loss hits their bottom line. Fraud that is perpetrated against a company's bank account typically occurs through check, ACH or wire fraud - online and offline. Responsibility for fraud prevention is shared between the company and their partners, including their bank. The best way to protect your business against fraud is to have a plan in place before it occurs. This is an introduction to the facts and possible solutions to help safeguard your company from malware and bank account fraud. Below are types of common fraud. We encourage you to contact your relationship manager for an in-depth discussion about preventative measures for your business.

Checking Fraud: Counterfeit or altered checks, and forged signatures comprise the main categories. Accounts payable/ disbursement accounts are the most frequent targets. The second most frequent target of check fraud is from the payroll account.

Wire Fraud: When an unauthorized individual performs a wire transfer to an unauthorized account.

ACH Fraud: When a client's account is accessed for unauthorized ACH payments. Businesses that originate their own ACH transactions online can be a fraudsters target.

Internet Fraud: This takes several forms and is intended to intercept, view or redirect confidential information about a business and its financial information in order to compromise accounts and commit fraud.

How To Protect Your Company

Online banking and automated cash management services provide a great amount of convenience for businesses – enabling you to make deposits, view account balances, wire funds and make ACH payments to keep your business running efficiently. By implementing a combination of internal controls, standardized operating procedures and fraud control services offered by Park Bank, businesses can minimize the risk of hacker attacks and internal fraud.

Basic Internal Controls for protection of your online payments and cash management data:

- Segregate responsibilities and utilize dual control for payments, template maintenance, payment entry and payments approval
- Use multi-factor authentication tools such as tokens, digital certificates and out-of-band authentication
- Delete online user IDs as part of the exit procedure when employees leave
- Use strong passwords (different passwords for different applications)
- Require passwords be changed regularly
- Shred account statements and other account documentation
- Secure check stock in locked storage
- Use high security check stock
- Convert paper payments to electronic delivery wherever possible
- Segregate duties for creating, approving and releasing wires with dual control
- Monitor and reconcile accounts daily
- Conduct surprise audits and fraud training for employees
- Mask account and Tax ID numbers in emails

PARK BANK
first IN LASTING RELATIONSHIPS®

- Keep antivirus and antispyware up-to-date
- Apply all Microsoft security patches
- Install a firewall to help prevent unauthorized access to your computer/ network
- Do not use work computers for risky or non-work applications (games, file sharing, personal email accounts)
- Perform background checks on employees during the hiring process
- Back up your files on a regular basis
- Educate employees on the dangers of:
  - Opening attachments and links from unkown senders
  - Visiting websites and clicking on photos, documents and videos that are publicly posted
- Never share any confidential information, especially social security numbers, Tax IDs, or account numbers via email. Park Bank will never ask for confidential information via email.

How Park Bank Can Help

At Park Bank, we use advanced Internet security, data encryption and other various security measures to help keep your accounts safe. Online account access uses multi-factor authentication for login and automatic logoff for your protection. In addition, Park Bank offers a variety of services to support your company's internal controls and processes.

Secure Token Login with Out-of-Band Authentication: This service provides increased security protection to Business Online Banking users during the login process by providing time-synchronous, one-time password authentication. Each authorized user is issued a device, called a digital token, which contains a six-digit number that uses a proven algorithm to generate a new one-time password every 30 seconds. To log in, a user enters the six-digit number that appears and an eight-digit user pass code, both of which confirm the user's identity. In addition to tokens, Business Online Banking verifies many factors to the user's typical login behavior and if necessary, an automated phone call will be generated to the number on file for that user. All businesses that utilize the ACH and Wire module within Business Online Banking are required to use Secure Token Login to protect their systems from fraudulent access to their account information. A small device is assigned to each user.

Positive Pay: This service provides check reconciliation and helps prevent fraud by identifying discrepancies between checks presented to Park Bank for payment and those issued by your company before the items are paid against your account.

Account Reconciliation: For companies that write a large volume of checks, need to track a high volume of deposits or have multiple deposit sources, this service enhances audit control and reduces clerical time spent on account reconciliation.

ACH Debit Block/Filler/Positive Pay: This highly flexible service allows a company to decide which debit transactions should be blocked or automatically posted based on a number of filtering options. This helps protect business accounts from unauthorized or fraudulent ACH debit entries.

Contact your Relationship Manager or a Treasury Management representative at 414.466.8000 for a fraud review.

PARK BANK
first IN LASTING RELATIONSHIPS®