Fraud Prevention and Risk Management for Your Business

What can you do to protect yourself?

Dual Control
Assign one user with the authority to create a transaction and choose a different user to actually submit / approve the transaction.

Tokens
An additional security feature in the form of a small, hand-held device that provides a unique password with each touch of the button. Howard Bank utilizes tokens provided by VASCO.

Multi-Factor Authentication
Some online applications require more than one layer of authentication before allowing the user access. For example, entering a user name and password is one layer of authentication. A second layer would be the requirement that you register your computer during the initial log in. If you sign-on from a different computer, you will be asked challenge questions before being allowed to continue.

Dedicated Workstation
Designate a specific workstation as the "banking workstation" and limit its use to only banking business. This workstation should not be used for web browsing.

Monitor and Balance Your Account Daily
You are the first line of defense against fraudulent activity on your accounts. Make it a practice to log onto your bank's website daily and review your accounts. Pay special attention to suspicious or unexplained transactions.

Always Update Workstations with Latest Anti-Virus Software
Advances in technology happen at lightning speed, as do the number of ways someone can wreak havoc on your accounts and computers. Make sure your anti-virus software and patches are up to date.

How does Reg E protect my business accounts?

The short answer is - IT DOESN'T!

Regulation E or the Electronic Funds Transfer Act is specifically geared towards consumers not businesses. This regulation provides the framework of the rights, liabilities and responsibilities for users of the Electronic Funds Transfer system. It covers:

- ATM Transfers
- Telephone bill payment systems
- Point of Sale (POS) terminal transfers in stores
- Pre-authorized transfers from or to a consumer's account (e.g. direct deposit)

HOWARD BANK

What are some ways you can mitigate your own risk for cyber attacks?

Positive Pay - Ensure only the checks you write are being cashed.

Positive Pay was created to help prevent fraud on business checking accounts. As checks are issued, the payee name, check number, date and amount are entered in an online banking application. As those checks clear through the bank, they are matched up against the initial information entered by the customer. If there are any discrepancies between the actual check and the information entered, the check is considered an "exception item" and the customer is notified through the online banking application. This notification allows the customer to decide whether to pay or return the potentially fraudulent item.

Do Not Share Your Passwords

- Never share your password with anyone! Anything that happens under your login is automatically your responsibility.
- If one employee leaves and another is hired, be sure to terminate the departing employee's access and assign a new user ID for the new employee.
- Always contact Treasury Management when an employee, who had access to Online Banking, leaves your company. The Treasury Management department has the ability to block, delete and add users at your discretion.

Change Passwords

- Institute the practice of changing passwords every 30 – 90 days.
- Require minimum length and complexity of passwords.
- You should require passwords be between 8-16 characters, be alpha-numeric (a combination of both letters and numbers) and be case-sensitive.

Always lock workstations if leaving them unattended.

- Locking workstations will prohibit unauthorized users from gaining access to programs on your workstation when you are not around.

Always log out of internet sites that you visit.

- Don't just "X" out of the web browser screen when leaving an internet site. In most instances, the site will still "show" you as logged in, leaving the possibility for a non-authorized user to access the information.

Never download unauthorized shareware programs or files without authorization.

- Never download programs without first verifying the validity of the information.

E-mails are like postcards. ANYONE CAN READ THEM!

- Do not e-mail proprietary information without encrypting software.

When will the bank contact you requesting login or account information?

Plain and simple...never. Howard Bank will NEVER call you requesting your Online Banking login information or your account numbers. If you receive unsolicited calls requesting this information, hang up and contact the bank immediately.

Who can you call to report an issue or ask a question?

Treasury Management Service Line 410-735-2003
Bank Representative 410-750-0020
TreasuryManagement@HowardBank.com

HOWARD BANK