Business Identity Theft and Corporate Account Takeover Risk Assessment

First National Bank of Hereford encourages business customers to perform a self-assessment of risks associated with computer systems and business practices within their own systems. Include an assessment of the risks associated with the following systems and other information technologies that may apply, as well as mitigating controls that are in place to minimize or prevent the risks:

Internet Usage

- Is a firewall utilized?
- Is an anti-virus protection provided?
- Are employees allowed to "surf" the internet?
- Does the company maintain a web page?
- Are employees allowed to visit social networking pages?

Electronic Mail

- Is an anti-phishing system employed?
- Are employees allowed to access personal email accounts?
- Is there a prohibition on sending non-personal company information, such as bank account numbers by unsecured email?

Business Practices

- Are procedures utilized that require dual control over important functions?
- Are employee duties clearly defined by job description?
- Are employees required to swap duties?

The underlying purpose for the self-assessment is to determine where weaknesses exist and to identify controls that may help mitigate these risks.

Corporate Account Takeover

Corporate Account Takeover is the business equivalent of personal identity theft. Hackers, backed by professional criminal organizations, are targeting businesses to obtain access to their web banking credentials or remote control of their computers. These hackers will then drain the deposit and credit lines of the compromised bank accounts, funneling the funds through mules that quickly redirect the monies overseas into hackers' accounts.

As a business owner, you need an understanding of how to take proactive steps and avoid, or at least minimize, most threats.

- Use a dedicated computer for financial transactional activity. DO NOT use this computer for general web browsing and email
- Apply operating systems and application updates (patches) regularly
- Ensure that anti-virus/spyware software is installed, functional and is updated with the most current version
- Have host-based firewall software installed on computers

- Use latest versions of Internet browsers, such as Explorer, Firefox or Google Chrome with "pop-up" blockers and keep patches up-to-date
- Turn off your computer when not in use
- Do not batch approve transactions; be sure to review and approve each one individually
- Review your banking transactions and your credit report regularly
- Contact your Information Technology provider to determine the best way to safeguard the security of your computers and networks

Call us immediately at **806.363.2265** if you believe that your First National Bank of Hereford account has been compromised or you feel you need to consider additional authentication options.