Bank of York Customer Information Security Awareness Program

INTRODUCTION

The Federal Financial Institutions Examination Council (FFIEC) has issued supervisory guidance designed to help make online transactions more secure. The guidance is in response to an ever more dangerous online threat environment. Scams and hacking techniques are more sophisticated, new threats are continually being developed and organized crime groups both in the United States and internationally have become a major force in expanding online fraud and theft.

Bank of York and your Log-In Credentials

We will never call, email or otherwise contact you to request your access ID, password, or other log-in credentials for the online services we offer. If you receive such a request, do not provide any information.

REPORTING SUSPICIOUS ACTIVITY

If you see suspicious activity on your account(s) or have received a suspicious call, email, letter or other similar contact regarding your relationship to Bank of York, call (205)392-5205 or toll free at (877)392-5205.

PROTECT YOURSELF BY CONTROLLING ONLINE RISKS

While online banking is safe, as a general rule you should always be careful about giving out your personal financial information over the Internet. Review the following tips to protect your personal information while using the Internet.

- Regularly log into your online accounts to verify that your bank, credit, and debit card statements and transactions are legitimate.

- Be suspicious of any e-mail with urgent requests for personal financial information.

- If you receive an unsolicited e-mail from any source asking you to click on a link to visit a site and input personal data, be very wary of it.

- Be cautious about opening any attachments or downloading any files from e-mails, regardless of who sent them.

- Instead of clicking on links in emails, type in the URL that you're familiar with, such as www.bankyork.com or select the Web address saved in your browser's "Favorites".

- If an offer sounds too good to be true, it probably is and should be avoided.

- If you have any doubts about the validity of an email, contact the sender using a telephone number you know to be genuine.

- Before you initiate an online transaction, make sure your personal information is protected by looking for indicators that the site is secure. URLs for secure sites typically begin with "https" instead of "http" and display a lock in the lower right corner of your browser.

- Use anti-virus software and keep it up-to-date.

- Make sure you have applied the latest scurity patches for your computer. Most software providers, like Microsoft, offer free security patches.

- If you have broad-band Internet access, such as cable modem or DSL, make sure that you have a firewall. We take numerous steps to keep your account information secure. However, you must take precautions as well.

- **Choose a good passcode** - Your online passcode, along with your access ID, authenticate your identity when accessing online accounts. You should carefully select a passcode that is difficult to guess and not use personal information or a word that can be found in the dictionary.

- **Keep your passcode safe** - Even the best passcode is worthless if it's written on a note attached to your computer or kept in your checkbook. Memorize your passcode and never tell it to anyone.

- **Change your passcode regularly** - It's important to change your passcode regularly.

- **Remember to log off properly -** You may not always be at your own computer when banking online. Therefore, it's important to log off using the "log off" link at the top of each Internet banking page. If you forget to do so, the system automatically signs you off after 10 minutes of inactivity.

CONSUMER PROTECTION – REGULATION E

Regulation E provides rules for error resolution and unauthorized transactions for electronic fund transfers, which includes most transactions processed online. In addition, it establishes limits to your financial liability for unauthorized electronic fund transfers. These limits, however, are directly related to the timeliness of your detection and reporting of issues to Robertson Banking Company. It is for this reason that we encourage you to immediately review periodic account statements and to regularly monitor your account activity online.

The "Electronic Fund Transfers" disclosure provided to you at the time of account opening provides detailed information. We will provide to you, upon request, a free printed copy of this disclosure.

Web Resources – Learn more and do more to protect yourself online!

http://www.stopthinkconnect.org

Consumer Alerts and online security tips on the FTC website

http://ftc.gov/bcp/menus/consumer/data/privacy.shtm

Scams and Fraud and tips to avoid becoming a victim- Go to FBI website

http://www.fbi.gov/scams-safety/

R**ecent scams and how to report scams** - Go to the IC3 website, a partnership of the FBI, the National White Collar Crime Center, and the Bureau of Justice:

http://www.ic3.gov/default.aspx

ADDITIONAL INFORMATION FOR BUSINESS USERS OF ONLINE SERVICES

The new FFIEC Guidance takes note that business transactions, because of their frequency and dollar value, are inherently more risky than consumer transactions. The Guidance also notes the steep rise of online account takeovers and unauthorized online fund transfers related to business accounts in the last five years.

Recently, small- to medium-sized businesses have been primary targets as cyber criminals have recognized that the security controls they have in place are not as robust as that of larger businesses. Analysis indicates enhanced controls over administrative access and functions related to business accounts and layered security using multiple and independent controls would help to reduce these types of crime.

The FFIEC Guidance suggests enhanced controls for businesses:

Business customers should be encouraged to perform a **periodic risk assessment and an evaluation of the effectiveness of the controls they have in place** to minimize the risks of online transaction processing.

The protecting yourself by controlling online risks tips above provide a starting point for this process and the web resource links provide additional detailed information.

http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf

The FTC Business Center has a great deal of information for businesses at

http://business.ftc.gov/privacy-and-security/data-security

Business customers should **understand the security features of the software and websites they utilize and take advantage of these features.** Segregation of duties—the process of separating duties so no one person can perform all steps of a transaction—is an example of a very important security feature.

Layered security options that may be available to business customers doing online transactions include transaction thresholds, out-of-band verification (such as telephone or email verifications), fraud detection and monitoring systems, and IP reputation–based services. The Guidance encourages establishing layered security processes.

Please remember to contact Bank of York if you should have any concerns or questions.

Bank of York – Main Office
PO Box 96
York, AL. 36925
205-392-5205
dpmanager@bankyork.com

Bank of York – Livingston Branch
716 N. Washington St.
Livingston, AL. 35470
205-652-1391