FFIEC CONSUMER GUIDANCE

MULTI-FACTOR AUTHENTICATION AND LAYERED SECURITY

>>>Online Security Is Our Top Priority!<<<

New supervisory guidance from the Federal Financial Institutions Examination Council (FFIEC) will help banks strengthen their vigilance and make sure that the person signing into your account is actually you.

UNDERSTANDING THE FACTORS

Authentication factors generally involve one or more basic factors:

- Something the user KNOWS (e.g., password, PIN)
- Something user HAS (e.g., debit card)
- Something the user IS (e.g. biometric characteristic, such as fingerprint)

Multi-factor authentication uses more than one method, and thus is considered a stronger fraud deterrent.

To assure your continued security online, your bank uses both single and multi-factor authentication, as well as additional "layered security" measures when appropriate.

LAYERED SECURITY FOR INCREASED SAFETY

Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. An example of layered security might be that you follow one process to log in (user/password), and then give additional information to authorize funds. Layered security can substantially strengthen the overall security of online transactions.

INTERNAL ASSESSMENTS AT YOUR BANK

On the back-end, the new supervisory guidance offers ways your bank can look for anomalies that could indicate fraud. The goal is to ensure that the level of authentication called for in a particular transaction is appropriate to the transaction's level of risk. Accordingly, your bank has concluded a comprehensive

risk-assessment of its current methods as recommended in this supervisory guidance. These risk assessments consider, for example:

- changes in the internal and external threat environment
- changes in the customer base adopting electronic banking
- changes in the customer functionality offered through electronic banking; and
- actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry.

Whenever increased risk to your transaction security might warrant it, your bank will be able to conduct additional verification procedures, or layers of control, such as:

- Utilizing call-back (voice) verification
- Employing customer verification procedures, especially when opening accounts online.
- Analyzing banking transactions and log in patterns to identify suspicious patterns.

YOUR PROTECTIONS UNDER "REG E"

Regulation E provides protection to consumers from losses that involve electronic transactions (including Internet banking losses). The level of protection provided depends on how quickly losses are detected and reported to the bank.

CUSTOMER VIGILANCE: THE FIRST LINE OF DEFENSE

Understanding the risks and knowing how fraudsters might trick you is a critical step in protecting yourself online. You can make your computer safer by installing and updating regularly your

- Anti-virus software
- Anti-malware programs
- Firewalls on your computer
- Operating system patches and updates

You can learn more about online safety at these websites:

www.staysafeonline.com
www.ftc.gov

www.usa.gov
www.idtheft.gov

IF YOU HAVE SUSPICIONS

If you notice suspicious activity within your account or experience security-related events, contact Oklahoma Bank & Trust at 580-323-2345.