

Important Facts About Your

Account Authentication & Online Banking



◆ Multi-factor authentication and layered security are helping ensure safe Internet transactions for banks and their customers.

Online Security Is our Top Priority!

If you use online or mobile banking, you will be interested to learn that six federal financial industry regulators teamed up recently to make your accounts more secure. 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. The supervisory guidance is designed to make online transactions of virtually all types safer and more secure.

◆ UNDERSTANDING THE FACTORS

Online security begins with the authentication process, used to confirm that it is you, and not someone who has stolen your identity. Authentication generally involves one or more basic factors:

- Something the user knows (e.g., password, PIN)
- Something the user has (e.g., VISA Check Card, token)
- Something the user is (e.g., biometric characteristic, such as a fingerprint)

Single factor authentication uses one of these methods; multi-factor authentication uses more than one, and thus is considered a stronger fraud deterrent. When you use your ATM, for example, you are utilizing multi-factor authentication: Something you have, your VISA Check Card and something you know, your PIN.

To ensure your continued security online, First Bank & Trust Company 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 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 transfers.

Layered security can substantially strengthen the overall security of online transactions... protecting sensitive customer information, lessening the chance of identity theft, and reducing account takeovers and the resulting financial losses.

◆ INTERNAL ASSESSMENTS AT YOUR BANK

The new supervisory guidance offers ways First Bank & Trust Company 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, First Bank & Trust Company 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, First Bank & Trust Company may also rely on several layers of control, such as:

- Utilizing call-back (voice verification), e-mail approval, or cell phone-based identification
- Analyzing banking transactions to identify suspicious patterns of activity
- Establishing dollar limits that require manual intervention to exceed a preset limit and complete the transaction.

◆ YOUR PROTECTIONS UNDER “REG E”

First Bank & Trust Company follows specific rules for electronic transactions issued by the Federal Reserve Board. Known as **Regulation E**, the rules cover all kinds of situations revolving around transfers made electronically. Under the consumer protections provided under **Reg E**, you may be able to recover internet banking losses according to how soon you detect and report them.

Here is what the Federal rules require: If you report the losses within two days of receiving your statement, you can be liable for no more than \$50. After two days, you can lose as much as \$500. After 60 days, you could be legally liable for the full amount.

For your protection, monitor your account frequently via Online Banking and immediately notify the bank of any unauthorized transactions.

◆ CUSTOMER VIGILANCE: THE FIRST LINE OF DEFENS

Of course, 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 use the “Alerts” function to get an e-mail notification when your balance drops to a certain dollar amount or when an ACH charge, such as your electric bill payment, comes in on your account.

You can also learn more about online safety and security at these websites:

- www.staysafeonline.com
- www.ftc.gov
- www.usa.gov
- www.idtheftcenter.org

◆ IF YOU HAVE SUSPICIONS

If you notice suspicious activity within your account or experience security-related events (such as a Phishing mail from someone claiming to be from the bank), please contact the Electronic Banking department at 276-623-2323 ext. 240 or by e-mail to info@firstbank.com



Bank & Trust Co.
The Bank That Puts You First
www.firstbank.com
Member FDIC