ELECTRONIC BANKING & LAYERED SECURITY

FOR ONLINE BUSINESS TRANSACTIONS

New financial standards will assist banks and business account holders to make online banking safer and more secure from account hijacking and unauthorized funds transfers.

Banks and Businesses Team Up for Security

As someone responsible for a business bank account, you will want to know that new supervisory guidance from the Federal Financial Institutions Examination Council (FFIEC) is helping banks strengthen their vigilance and ensure that your business accounts are properly secured during money transfers of all kinds. FFIEC is the coordinating group that sets standards for the major financial industry regulators and examiners.

UNDERSTANDING THE RISKS

FFIEC studies have shown that there have been significant changes in the threat landscape in recent years. Fraudsters - many from organized criminal groups - have continued to deploy more sophisticated methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. For example, hacking tools have been developed and automated into downloadable kits, increasing their availability to less experienced fraudsters.

As a result, online account takeovers and unauthorized funds transfers have risen substantially each year since 2005, ***particularly with respect to commercial accounts,*** representing losses of hundreds of millions of dollars.

ENHANCED CONTROLS PROTECT HIGHER RISKS

The FFIEC supervisory guidance addresses the fact that not every online transaction poses the same level of risk. First Bank & Trust Company implements more robust controls as the risk level of the transaction increases.

Online business transactions often involve ACH file origination and interbank wire transfers. Since the frequency and dollar amounts of these transactions are generally higher than consumer transactions, they pose a comparatively *increased level of risk* to the customer and to the bank. First Bank & Trust Company implemented security plans utilizing controls consistent with the increased level of risk for covered business transactions.

These enhanced controls are designed to exceed the controls applicable to routine customer users. For example, a preventive control could include requiring an additional authentication routine such as a code from a token or answering a challenge question. A detective control might include a transaction verification alert immediately following the submission of a high dollar ACH transaction.

SUMMARY OF RECOMMENDATIONS FOR BUSINESS ACCOUNTS

- **First Bank & Trust Company urges business account holders to conduct periodic assessment of their internal controls**
- **For your protection, monitor your account frequently via Online Banking and immediately notify the bank of any unauthorized transactions**
- **Use layered security for system administrators**
- **Initiate enhanced controls for high-dollar transactions, for example time limits, dual-control, or e-mail alerts**
- **Provide increased levels of security as transaction risks increase**
- **Participate in "Positive Pay", so that the bank knows what checks you have written**

LAYERED SECURITY FOR INCREASED SAFETY

First Bank & Trust Company uses both single and multi-factor authentication, as well as additional "layered security" measures when appropriate.

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. This allows your bank to authenticate customers and respond to suspicious activity related to initial login...and then later to reconfirm this authentication when further transactions involve activity such as the transfer of funds.

For business accounts, layered security might often include **enhanced controls for system administrators** who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations. Enhanced administrative controls can effectively reduce money transfer fraud.

INTERNAL ASSESSMENTS AT YOUR BANK

The new supervisory guidance addresses the process of looking for anomalies that could indicate fraud. The goal is to ensure that the level of authentication is appropriate to the level of risk. Accordingly, First Bank & Trust Company has concluded a comprehensive risk-assessment of its current methods as recommended in the FFIEC guidelines. 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.

EXAMPLES OF LAYERED SECURITY FOR BUSINESS ACCOUNTS

Whenever increased risk to your transaction security might warrant it, your banker can advise you about additional layers of control, such as:

- **Fraud detection and monitoring** systems that include consideration of customer history and behavior;
- **Dual customer authorization** through different access devices;
- **"Positive Pay", debit blocks,** and other techniques to appropriately limit the transactional use of the account;
- **Transaction value thresholds**, batch total maximums, and allowable payment windows (e.g., days and times);
- **Internet protocol (IP)** restriction to identify the IP address associated with your business;
- **Policies and practices for addressing customer devices** identified as potentially compromised and customers who may be facilitating fraud;
- **Account maintenance controls** over activities performed by customers either online or through customer service channels.

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***. In general, these protections are extended only to consumers and consumer accounts. Under the protections provided under ***Reg E***, consumers may be able to recover internet banking losses according to how soon they are reported.

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

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