FFIEC Business Account Guidance

Risk Assessment & Layered Security

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) are helping banks strengthen their vigilance and assure 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, recommending that financial institutions implement more robust controls as the risk level of the transaction increases.

Online business transactions generally involve ACH file origination and frequent 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 institution and its customer, according to FFIEC. Thus banks are advised to implement 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 prior to final implementation of the access or application changes. A detective control might include a transaction verification notice immedi–ately following implementation of the submitted access or application changes. Based upon the incidents the Agencies have reviewed, enhanced controls over administrative access and functions can effectively reduce money transfer fraud.

Summary of recommendations for business accounts

- Banks to urge business account holders to conduct periodic assessment of their internal controls
- Use layered security for system administrators
- Initiate enhanced controls for high-dollar transactions
- Provide increased levels of security as transaction risks increase
- Offer customers multi-factor authentication

Layered security for increased safety

Your bank 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 generally 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 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.

Internal assessments at your bank

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 level of risk in that application. Accordingly, your bank 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.

Your bank joins FFIEC and the financial regulatory agencies in strongly urging businesses account holders to conduct similar internal assessments to ensure the highest level of security possible for your transactions.

Examples of layered security for business accounts

Whenever increased risk to your transaction security might warrant it, your bank will have available additional verification procedures, or 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;
- **Out-of-band verification** for transactions;
- **"Positive pay," debit blocks,** and other techniques to appropriately limit the transactional use of the account;
- **Transaction value thresholds,** number of transactions allowed per day, and allowable payment windows (e.g., days and times);
- **Internet protocol (IP) reputation-based tools** to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- **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"

Banks follow specific rules for electronic transactions issued by the Federal Reserve Board known as **Regulation E**. Under the protections provided under **Reg E**, consumers can recover internet banking losses according to how soon they are reported. In general, these protections are extended to consumers and consumer accounts.

If you have suspicions

If you notice suspicious activity within your account or experience security related events (such as a Phishing email from someone purporting to be from your bank), you can contact anyone at your bank and you will be quickly and courteously guided to the person responsible for such issues.