

Business Account Guidance

Important Facts about your Account Authentication and Online Banking



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

At Mascoma Savings Bank, the security of customer information is a priority. We are strongly committed to the safety and confidentiality of your records. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. One of the best ways to avoid fraud is to become an educated user.

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.

SUMMARY OF RECOMMENDATIONS FOR BUSINESS ACCOUNTS

- Business account holders should conduct periodic assessments 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
- Utilize a unique complex password (Upper Case, Lower Case, Special Characters) at least 8 characters long
 - DO NOT re-use passwords that you have registered for at other websites
 - Change your password every 30 days
- Watch out for copycat web sites that deliberately use a name or web address very similar to, but not the same as the real one. The intent is to lure you into clicking through to their web site and giving out your personal information, such as a bank account number, credit card number or online banking login information.

LAYERED SECURITY FOR INCREASED SAFETY

Mascoma Savings 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 Mascoma Savings 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.

INTERNAL ASSESSMENTS AT MASCOMA SAVINGS BANK

The new supervisory guidance offers ways Mascoma Savings 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, Mascoma Savings 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.

Mascoma Savings Bank joins FFIEC and the financial regulatory agencies in strongly urging business 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;
- **Out-of-band verification** for transactions;
- **Transaction value thresholds**, dollar amounts allowed per day
- **Internet protocol (IP) reputation-based tools** to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities

OTHER PROTECTIONS THE BANK TAKES

- We will never ask you for your online banking password
- All electronic communication is done through the secure email system provided within the online banking system.
- We will never send your non-public information via email unless it utilizes our encrypted email system.

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 you can contact Mascoma Savings Bank’s Internet Banking Support Line at 802-280-4228 or email at msbinfo@mascomabank.com.



**Mascoma
Savings Bank**

Member
FDIC

2/12x