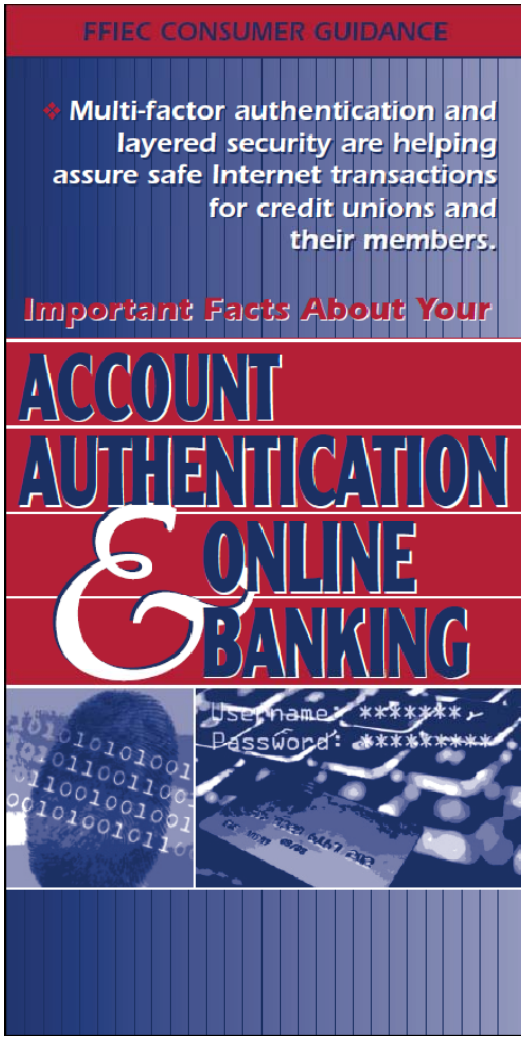
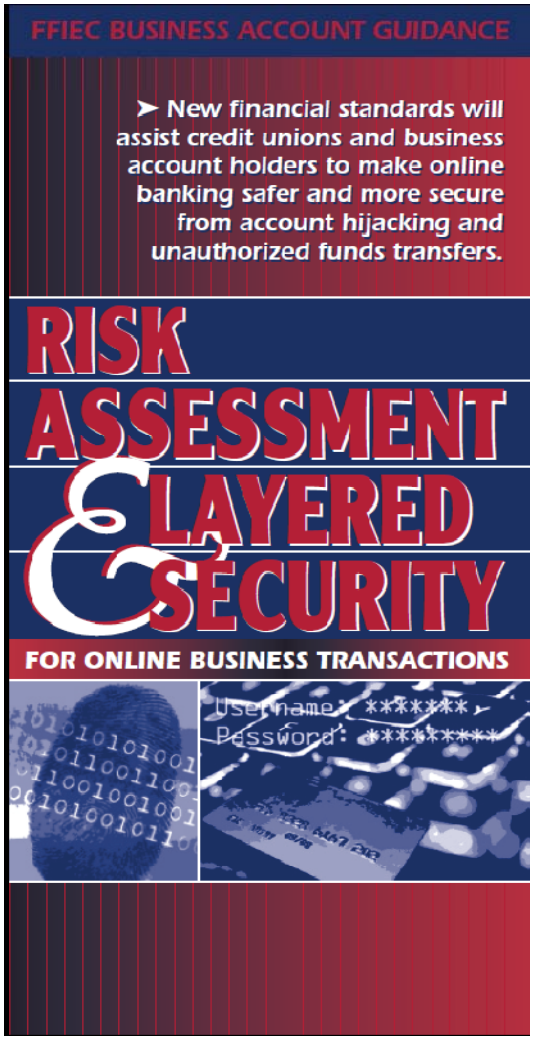
Online Protection





Here are two informational brochures that disclose ways that we protect your accounts and tips you can use to be safer online.

FFIEC BUSINESS ACCOUNT GUIDANCE

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

RISK ASSESSMENT & LAYERED SECURITY

FOR ONLINE BUSINESS TRANSACTIONS

Credit Unions and Businesses Team Up for Security

As someone responsible for a business credit union account, you will want to know that new supervisory guidance from the Federal Financial Institutions Examination Council (FFIEC) are helping credit unions 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 members' 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

SUMMARY OF RECOMMENDATIONS FOR BUSINESS ACCOUNTS

- Credit unions 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 members multi-factor authentication

institutions implement more robust controls as the risk level of the transaction increases.

Online business transactions generally involve ACH file origination and frequent intercredit union 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 member, according to FFIEC. Thus credit unions 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 member 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.

LAYERED SECURITY FOR INCREASED SAFETY

Your credit union 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 credit union to authenticate members 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 CREDIT UNION

The new supervisory guidance offers ways your credit union 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 credit union has concluded a comprehensive risk-assessment of its current methods as recommended in the FFIEC guidelines. These risk assessments consider, for example:

EXAMPLES OF LAYERED SECURITY FOR BUSINESS ACCOUNTS

Whenever increased risk to your transaction security might warrant it, your credit union will have available additional verification procedures, or layers of control, such as:

- **Fraud detection and monitoring** systems that include consideration of member history and behavior;
- **Dual member 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 credit union servers from IP addresses known or suspected to be associated with fraudulent activities;
- **Policies and practices for addressing member devices** identified as potentially compromised and members who may be facilitating fraud;
- **Account maintenance controls** over activities performed by members either online or through member service channels.

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

Your credit union 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.

YOUR PROTECTIONS UNDER "REG E"

Credit unions 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. Your credit union can provide additional details about how ***Reg E*** might affect your business account.

IF YOU HAVE SUSPICIONS

If you notice suspicious activity within your account or experience security-related events you can contact anyone at your credit union and you will be quickly and courteously guided to the person responsible for handling such issues.

© FINANCIAL EDUCATION CORPORATION

FFIEC CONSUMER GUIDANCE

❖ Multi-factor authentication and layered security are helping assure safe Internet transactions for credit unions and their members.

Important Facts About Your

ACCOUNT AUTHENTICATION & ONLINE BANKING

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 credit unions 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., ATM card, smart card)
- 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: Factor number one is something you have, your ATM card; factor number two is something you know, your PIN.

To assure your continued security online, your credit union 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 transfers.

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

The purpose of these layers is to allow your credit union to authenticate members and detect and respond to suspicious activity related to initial login and then to reconfirm this authentication when further transactions involve the transfer of funds to other parties.

INTERNAL ASSESSMENTS AT YOUR CREDIT UNION

On the back-end, the new supervisory guidance offers ways your credit union 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 credit union 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 member base adopting electronic banking
- changes in the member 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 credit union will be able to conduct additional verification procedures, or layers of control, such as:

- **Utilizing call-back (voice) verification,** e-mail approval, or cell phone-based identification.
- **Employing member verification procedures,** especially when opening accounts online.
- **Analyzing banking transactions to identify suspicious patterns.** For example, that could mean flagging a transaction in which a member who normally pays $10,000 a month to five different vendors suddenly pays $100,000 to a completely new vendor.
- **Establishing dollar limits that require manual intervention** to exceed a preset limit.

YOUR PROTECTIONS UNDER "REG E"

Credit unions follow 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 can 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 the first $50. After two days, the amount increases to $500. After 60 days, you could be legally liable for the full amount. These protections can be modified by state law or by policies at your credit union, so be sure to ask your credit union how these protections apply to your particular situation.

MEMBER VIGILANCE: THE FIRST LINE OF DEFENSE

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 also learn more about online safety and security 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 (such as a Phishing email from someone purporting to be from your credit union), you can contact anyone at your credit union and you will be quickly and courteously guided to the person responsible for such issues.

© FINANCIAL EDUCATION CORPORATION