# FFIEC ONLINE SECURITY GUIDANCE

## Important Information You Should Know About Online Security

If you use online banking or other internet banking services as a consumer or a business, you will be interested to learn that six federal financial industry regulators have recently joined forces to make your accounts even more secure. New supervisory guidance from the Federal Financial Institutions Examination Council (FFIEC) will help us strengthen our vigilance to assure that your accounts are properly secured and to make virtually all types of online transactions safer and more secure.

### Consumer Guidance: Account Authentication & Online Banking

Multi-factor authentication and layered security are helping guarantee safe Internet transactions for our customers and us.

### Business Guidance: Risk Assessment & Layered Security

New financial standards help us and our business account holders make online banking safer and more secure from account hijacking and unauthorized funds transfers.

### Authentication: Understand the Factors

The authentication process is of vital importance to verify that YOU, and not someone who has stolen your personal identity or hijacked your corporate account, is conducting your online transactions. Authentication usually involves one or more basic factors:

- Something the user KNOWS (such as a password or PIN)
- Something the user HAS (such as an ATM Card or Token)
- Something that the user IS (a biometric characteristic such as a fingerprint)

Single factor authentication uses one method. Multifactor authentication uses more than one method, and is a much stronger fraud deterrent.

### Internal Assessments at Your Bank

The new supervisory guidance offers ways we can look for irregularities that could indicate fraud. Geauga Savings Bank has conducted a comprehensive risk-assessment of its current methods with regards to the following:

- 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 the industry

Whenever an increased risk to your transaction security may warrant it, we will be able to conduct additional verification procedures or layers of control such as:

- Utilizing call back (voice) verification, email approval, or cell phone based identification
- Employing customer verification procedures
- Analyzing banking transactions to identify suspicious patterns
- Establishing dollar limits that require manual intervention to exceed a preset limit

### Your Protection Under "Reg E"

We are required to follow specific rules issued by the Federal Reserve Board, known as Regulation E, for electronic transactions. Reg E covers 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.

### What the Federal Rules of Reg E require:

If you report the losses within two (2) days of receiving your statement, you can be liable for the first $50. After two (2) days, the amount you can be liable for increases to $500. After sixty (60 days) you could be liable for the full amount. Details of your rights are included on each account statement.

### Understand the Risks

FFIEC studies show significant increase in cyber threats. Not only do fraudsters continue to deploy more sophisticated methods to compromise security measures, they now manufacture computer hacking kits to sell illegally to less experienced fraudsters.

Geauga Savings Bank
10800 Kinsman Road • Newbury, OH 44065
440-564-9441 • www.GeaugaSavings.com

# FFIEC ONLINE SECURITY GUIDANCE

Important Information You Should Know About Online Security

## Corporate Account Takeover (CAT)

Corporate Account Takeovers have increased every year, representing losses of hundreds of millions of dollars. When a Corporate Account Takeover (CAT) occurs, computer hackers steal legitimate login credentials, and fraudulent transfers (ACH or Wire Transfers) are completed before the business account owner knows what happened.

## 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 area is compensated by strength in another control area.

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

The purpose of these layers is to allow us to authenticate customers and detect and respond to suspicious activity related to initial login and then to reconfirm this authentication when further transactions involve transfers of funds or higher risk actions.

## Examples of Layered Security for Businesses

For business accounts, layered security can include enhanced controls for system administrators who are granted privilege to set up or change system configurations, and control access privileges and application functions or limitations for their own staff and users. Added layers can include:

- Fraud detection and monitoring systems that include consideration of your transaction history and behavior
- Dual customer authorization through different access devices
- Out-of-band verifications for certain transactions
- "Positive Pay" debit blocks or other techniques that limit transactions
- Transaction value thresholds that restrict the number or amount of transactions for a set time frame
- Internet Protocol (IP) reputation-based tools
- Policies and procedures for addressing customerdevices that have been potentially compromised, or for detecting customers who may be facilitating fraud
- Account maintenance controls over activities performed online or through customer service channels

## Recommendations for Business Accounts

- Conduct periodic assessments of internal controls
- Use layered security for system administrators
- Initiate enhanced controls over high-dollar transactions
- Provide increased levels of security as transaction risk increase

## Customer Vigilance

Knowing how fraudsters may try to trick you and understanding the risks is critical to safe online banking. You can take further steps to protect yourself and make your computer safer by installing and regularly updating:

- Anti-virus software
- Anti-malware programs
- Firewalls on your computer
- Operating system patches and updates

Additional steps include:

- Create strong complex passwords that contain both CAPITAL and small letters, numbers and any allowed special characters
- If you think you may have visited a website with malware or if you think your computer may be infected with a virus, do not access your online banking or other sensitive logins until you have scanned your computer and know it is clean and virus free

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 a security related event (such as loss of token, compromised PIN or Password, known or suspected infection of computer or network by viruses or malware, etc) please contact us immediately, and you will be quickly and courteously directed to a customer service representative who can assist you with these matters.

Geauga Savings Bank
10800 Kinsman Road • Newbury, OH 44065
440-564-9441 • www.GeaugaSavings.com