

## Protections under Regulation E

Regulation E, better known as the Electronic Fund Transfer Act (EFTA), established the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer (EFT) services and of credit unions that offer these services.

An EFT is any transfer of funds that is initiated through an electronic terminal, telephone or computer for the purpose of ordering, instructing, or authorizing a debit or credit to your account(s).

## Examples of EFTA covered electronic services offered by GEMC FCU:

1. ATM (Automated Teller Machine)
2. Debit Card Transactions (Point-of-Sale)
3. Powerline (Telephone Audio Response)
4. ACH (Automated Clearing House)
5. Online Banking/Bill Pay

For more information on your rights, responsibilities and liabilities under EFTA, please review your GEMC FCU membership booklet - Electronic Fund Transfer Agreement and Disclosure.

## Additional Resources:

[www.staysafeonline.com](http://www.staysafeonline.com)

[www.ftc.gov](http://www.ftc.gov)

[www.usa.gov](http://www.usa.gov)

[www.idtheft.gov](http://www.idtheft.gov)

[www.onguardonline.gov](http://www.onguardonline.gov)



## GEMC FCU Contact Information

If you suspect or notice any suspicious account activity or experience any information security related events with GEMC's online banking, contact us IMMEDIATELY at:

Monday through Friday 9am – 4pm (excluding holidays):  
Tucker Branch Phone: 470-514-3000  
Dallas Branch Phone: 770-445-2800  
Douglasville Branch Phone: 770-949-3557

After hours and holidays (card fraud only):  
VISA Credit Card: 800-299-9842  
GEMC FCU Debit Card: 800-472-3272

GEMC Federal Credit Union  
2100 East Exchange Place, Suite 101, Tucker, GA 30084

Your online security is very important to us. We take several precautions to ensure your information is secure.

To access our secure area, you must enter your Logon ID and Security Code. In addition, Enhanced Authentication provides extra protection for your online data and helps guard against phishing scams and identity theft by recognizing your computer and usage patterns.

If a questionable logon attempt is detected, the system will require additional identity verification before allowing access.

The system also displays a secret image and phrase combination that you choose. This secret image and phrase is displayed each time you log on to reassure you that you are logging on to your actual Internet banking or bill payment site. If you do not see your image and phrase, you should not enter your Security Code.

Other online security measures include:

- Secure Sockets Layer (SSL) protocol to ensure that your connection and any information transmitted is protected.
- 128-bit encryption to make your information unreadable as it passes over the Internet.
- Automatic time out that occurs if you are inactive in the secure area of our site for more than 10 minutes.



# Authentication In an Internet Banking Environment



GEMC Federal Credit Union (GEMC) is always committed to ensuring the safety of our member's information and GEMC FCU's internet banking environment is no exception. With more and more members using internet banking, unscrupulous individuals are working harder than ever to find new ways to scam unsuspecting individuals. One of the best defenses against fraud is to remain educated on cyber-safety. GEMC FCU is dedicated to helping our members stay cyber-safe.

### Tips on keeping yourself safe in the internet environment:

- 1. KEEP INFORMATION PRIVATE:** Be extremely careful if you have to use a library or other public computer to access your account. Online fraudsters could have installed a keystroke logger to obtain your username, PIN, answers to your security questions, and your password.  
  
Fraudsters are known for masking emails and text messages to look like they come from a trusted sender. DO NOT send your account number or personal information via email or text messaging to anyone. DO NOT use a hyperlink that is located in an email to access GEMC FCU's online banking website – and always ensure that the web address starts with HTTPS.
- 2. ACCOUNT REVIEW:** GEMC FCU encourages members to log in to their accounts regularly to review account activity, even if you have not performed any recent transactions. Early detection is a key component to stopping fraud quickly. If there are any concerns, contact GEMC FCU immediately at 770-270-7851.
- 3. STRONG PASSWORD:** GEMC FCU encourages members to have a password that is at least 8 characters long with a mixture of upper and lower case letters, numbers, and special characters. Change your password regularly and do not give anyone your password or allow anyone else to use your password.
- 4. ENHANCED AUTHENTICATION:** Online theft is a serious concern. At GEMC FCU, we have implemented enhanced levels of authentication that adds additional security to our internet banking/bill pay platform that

will better protect our members from falling victim to internet crimes. Whenever you log on to GEMC internet banking you will see your image and phrase so you know you are accessing the GEMC internet banking internet site - and not a bogus site.

- 5. While GEMC FCU continues to evaluate and implement the latest improvements in Internet security technology, users of the system also have responsibility for the security of their information and should always follow the recommendations listed below:**
  - Utilize current versions of Microsoft Internet Explorer, Firefox, or Netscape browsers.
  - Keep your Security Code confidential.
  - Be sure others are not watching you enter information on the keyboard when using the system.
  - Never leave your computer unattended while logged on to the system. Others may approach your computer and gain access to your account information if you walk away.
  - Exit the system when you are finished to properly end your session. Once a session has ended, no further transactions can be processed until you log on to the system again.
  - Close your browser when you are finished, so that others cannot view any account information displayed on your computer.
  - Keep your computer free of viruses. Use virus protection software to routinely check for a virus on your computer. Never allow a virus to remain on your computer while accessing the system.
- 6. ASSESS YOUR OWN RISKS:** GEMC FCU encourages every member to do their own risk assessment on their online banking security controls such as, but not limited to: Storage of online banking information (account number, password, PIN, and answers to security questions).

### GEMC FCU initiating contact with you:

- GEMC FCU employees will NEVER call, email, or send you a text message asking for any of your electronic banking credentials. GEMC FCU may inquire about your electronic banking credentials if you initiate contact and express online banking problems.
- Card fraud detection MAY contact you on behalf of GEMC FCU to verify unusual credit or debit card transactions. Card fraud detection will NEVER ask you for any of your electronic banking credentials. Card fraud detection will:
  - Identify themselves as card fraud detection and state they are calling on behalf of GEMC Federal Credit Union.
  - Card fraud detection WILL give you the last four digits of the card number they are contacting you about. DO NOT give anyone claiming to be card fraud detection your full card number, expiration date, three digit security code (located on the back of your card) or your full social security number.
  - Card fraud detection WILL ask you to verify the transactions(s) in question.
  - Card fraud detection MAY ask you for information about your address or last four of your social security number.
  - Card fraud detection WILL only ever call you about credit or debit card transactions.