What is EnFact?

At GHA Federal, our goal, quite simply, is to minimize your exposure to risk and the impact of any fraudulent activity on your accounts.
To protect your accounts, GHA Federal monitors debit card transactions for potentially fraudulent activity through a Fraud Detection Program called EnFact. Potentially fraudulent activity may include a sudden change in locale (such as when a U.S. issued card is used unexpectedly overseas or in a foreign country), a sudden string of costly purchases, or any pattern associated with new fraud trends around the world.
If we suspect fraudulent debit card use, our monitoring agency will be calling you to validate the legitimacy of your suspect transactions.

We may be calling you...

If fraudulent debit card use is suspected on your bank account, you will be called to validate the legitimacy of your transactions. Your participation in responding to our call is critical to prevent potential risk and avoid restrictions we may place on the use of your debit card.

- Our automated call center will ask you to verify recent transaction activity on your card.
- You'll be asked to verify your identity and provide your 5 digit ZIP code.
- You'll be able to respond via your touchtone keypad.
- You'll also be provided a toll-free number to call should you have additional questions.

To ensure we can continue to reach you whenever potential fraud is detected, please keep us informed of your correct phone numbers (home, work and cell) and address at all times.
It is the policy of GHA Federal to NEVER solicit customer information or identification, numbers or passwords via e-mail. If you are approached with such an offer, do not reply to the e-mail and instead contact GHA Federal immediately.

Protect Yourself

A. Unless absolutely required for a legitimate business purpose, avoid giving:

- Address and Zip Code
- Phone Number
- Date of Birth
- Social Security Number
- ATM, Debit or Credit Card or Bank Account Number
- ATM, Debit or Credit Card Expiration Date

B. In stores and at ATMs, always cover your bank card and PIN and watch for:

- Cell phone cameras, mirrors or other tools used to view cards and PINs

- People watching your transactions
- Cashiers taking your card out of sight; instead take it to the register yourself
- Any unusual activity at ATMs; if you feel uncomfortable, go to another ATM
- Any device or coverings on the card slots of ATMs; if you see this do not insert your card and instead go to another ATM

C. Online, you should never respond to unsolicited e-mails that

- Ask you to verify your credit or debit card or bank account number; such e-mails are not sent by legitimate businesses
- Links to websites; such sites can look legitimate but may collect data or put spyware on your computer.