AmFirst ALERTS

Frequently Asked Questions

1. **What are AmFirst Alerts?**
   AmFirst is introducing a powerful new service to help protect our members' debit cards from fraudulent transactions. On November 5, we will launch *AmFirst Fraud Alerts*. This program will take the place of our current debit card fraud monitoring. The new program will be more flexible, intuitive and will give members better control over their debit cards than with our current fraud detection software. It will allow two-way messaging between AmFirst and members in near real time – what this means is members will receive a text alert asking if a suspected fraudulent transaction is authorized or not. If so, the card will remain active. If not, the card will be blocked immediately.

2. **Who will receive alerts?**
   All members with an open AmFirst debit card.

3. **What do I need to do?**
   Just use your card as normal and look out for alerts. Once you receive an alert, make sure the information included on it is accurate. It is important that we have your correct contact information on your account in order to best protect you from fraudulent card activity.

4. **How will I receive the alerts?**
   We will attempt to contact you using text messages, emails and phone calls. You must have a valid mobile phone number, home phone number and email address with AmFirst.

5. **What if I experience fraud?**
   You may respond with "NO" if you receive a text alert asking if a transaction was authorized by you. This will block the card. If you experience fraud, contact the number on the fraud alert to resolve your fraudulent transaction.

6. **What number will the text messages and phone calls come from?**
   The SMS text alerts will come from the number **47334 (*AmFirst Alerts*)**. Phone calls will come from **(844) 331-9932.** Be sure to save both of these numbers in your contact list so you will recognize them when they call.

7. **What email address will the email messages come from?**
   Alerts@Amfirst.org

8. **What email address will alerts go to?**
   Emails will go to the primary email address we have on our system currently associated with your account. **Can I respond to an email to deactivate my card due to fraud?**

No. Emails are a one-way communication channel. They are intended to be informative and notify you of possible fraud. You must respond to the text message you received or call the number on the email to resolve the fraudulent activity on your account.

9. **What phone number will alerts go to?**
   The text alerts will be sent to the phone number listed as your mobile number on your checking account. Automated voice calls will go to the number listed as the home number on your account. In many cases, you may receive a call and text alert if we detect fraud on your debit card.

10. **Can I receive text alerts on multiple phone numbers?**
    No. Only one mobile number can be linked to an individual user. We use the primary member's mobile number listed on your account.

11. **I don't want calls to my home phone. Can I have the phone notifications sent to my mobile phone?**
    Yes. Please call our Call Center (205-320-4000 or toll-free 1-800-633-8431) to request your contact information be updated.

12. **What information will the alerts include?**
    SMS text alerts will contain the merchant name, dollar amount in most cases, and the last 4 digits of your debit card. The message will ask, "Did you authorize". You should respond with a "YES" or "NO".

13. **What happens if I do not respond to the text alert or automated voice call I receive?**
    We will treat the suspected transaction as fraud and block your card from further use until we hear from you. There may be times when we may leave the card active until we hear from you.

14. **Why do some alerts not show the dollar amount or show an amount different than what I expected?**
    Some merchants, such as gas stations, hotels, car rental agencies, etc. send over an authorization amount to make sure the card is valid. After the transaction is final, the dollar amount is likely to be different. For example, a gas station may choose to send an authorization amount of $1 (or $100), but your actual gas purchase was $17.96. In some cases, we will notify you that a transaction was made with a "PENDING" dollar amount listed or the amount may reflect the amount the merchant sent to us to authorize.

15. **How long should it take to receive the alert?**
    Alerts usually arrive within a minute of the suspected transaction. However, timing could vary due to your mobile provider's network accessibility.

16. **What do I need to do if I get a suspected fraud alert?**
    If you receive a text alert asking you to verify a transaction, respond "Yes" or "No" to indicate if the transaction was authorized by you. If you receive an automated phone call, respond to the prompts appropriately. If you are alerted of a transaction that you did not make, call the

number on the alert immediately to speak to a representative and review your transactions to determine if any are fraud.

17. **Will I ever need to text personal information?**
    No. We will never ask you to text us your account number, personal identification such as your birthdate or Social Security number, or other personal information such as your mother's maiden name or address. If you ever receive a text message asking for your account numbers or other personal information, please do not respond.

Text Alert Examples:

General purchase alert message if fraud is suspected:

If you reply "**Yes**" to confirm an authorized transaction:

If you reply "**No**" to alert of an unauthorized transaction:

If AmFirst fraud alerts blocks your card due to fraud:

If your card is turned back on after being blocked:

Suspected Fraud Alert Email Sample:

AmFirst ALERTS

Dear John Smith,

For security purposes, we continuously monitor debit card transactions for possible fraudulent activity. The transaction indicated below has been identified as being suspicious. Please review the information and let us know if you authorized this transaction by calling (844) 331-9932

Reporting the transaction as unauthorized will disable your card in an effort to prevent additional fraudulent activity from occurring. We will contact you as soon as possible to provide further guidance related to the unauthorized transactions.

Card Ending: 5678
Transaction Date: Monday, September 17, 2018 8:44 AM
Merchant: GAS STATION X
Amount: $51.00

Some transactions are pre-authorized before the final sale. These can include purchases made at gas stations, hotels, and car rental merchants. Please note the amount shown above may not reflect the exact amount of your final transaction.

If we've already spoken to you about this matter, or you have already responded in another manner, please disregard this notice. No further action is required.

Thank you for choosing America's First Federal Credit Union