

FALCON FRAUD PROTECTION

We've got you covered, with Falcon Fraud Manager!

What is Falcon?

Falcon is fraud prevention software from FiServ, our debit card provider, which helps identify and reduce fraud risk by detecting potentially fraudulent PIN-based and signature-based debit transactions. It has a proven reputation of helping minimize payment card fraud losses.

How does Falcon work?

Falcon reviews how and where your card is being used and scores transactions based on transaction data and cardholder profile factors. Each transaction is given a score from one to 999, and the higher the score, the greater the likelihood that the transaction is fraudulent.

What happens if Falcon detects fraudulent activity on my debit card?

An automated FiServ Fraud system will call you if any suspicious card activity is detected on your account. They will identify themselves as First Farmers & Merchants Bank. If they are unable to reach you, they will leave a message with their contact information.

Falcon Fraud Manager maintains a 24/7 watch on your account. On high risk activity scenarios they will suspend activity immediately on your debit card until they can talk to you to determine if the risk is fraudulent activity or not. This process has saved our customers thousands of dollars in potential loss.

What information will I be asked for?

The automated system will ask you to verify your name and zip code. Once your address has been verified, they will then ask you to confirm your purchase activity. You will never be asked for your card number or PIN. If a transaction is not yours, you will be transferred to a Fraud Specialist.

Does this service cost anything for me?

No. First Farmers & Merchants Bank wants you to use your debit card with confidence. Falcon Fraud Manager is a FREE protection service available to you.

What if my debit card is declined at a merchant location?

One of the reasons may be that it was flagged as highly likely to be fraud, based on the way you typically use your card. If your transaction is declined for that reason, you will receive a phone call

from a Fraud Specialist to verify the transaction. If it was a legitimate transaction, the details will be made part of your card profile so that these types of transactions have a greater chance of being approved in the future.

What should I do if my card or transaction has been blocked by Falcon due to suspicious activity?

WE RECOMMEND SAVING THESE NUMBERS IN YOUR PHONE

**Contact a First Farmers & Merchants Bank representative.
Monday - Friday from 7:00 a.m. - 10:00 p.m.
Saturday from 7:00 a.m. – 5:00 p.m.
at 1-866-733-3444.**

**During after hours, you can contact the FiServ Fraud Specialist Department at
1-800-262-2024.**

(If they have left a message you will need the 6 digit personal message code)

How can I be proactive when using my debit card with Falcon Fraud Manager?

One thing to keep in mind is Falcon Fraud Manager will immediately block your card if it detects high scoring suspicious activity. A few tips to keep in mind are:

1. Always let FF&M Bank know when you plan to travel out of state and out of the country. This *can* help avoid potential blocks should your debit card be flagged for possible fraud.
2. Notify the bank immediately of any changes to your home, work or cell phone number. The Fraud Detection System will call the numbers on file with FF&M Bank.
3. In case your debit card is blocked from fraudulent transactions, we recommend always carrying multiple forms of payment with you.

Tips for preventing card fraud on your account...

- Memorize your PIN. Don't write it on your card or anything you carry near your card.
- Don't tell anyone your PIN or account number.
- Don't loan anyone your card.
- Report lost or stolen cards immediately. You may be liable for activity on your card if you do not report it as lost or stolen.
- Use caution when shopping online. Shop only at reputable merchants. Do not enter your card number unless the site is secure (https:)
- NEVER respond to a link or phone number in an e-mail message requesting personal information. Phishers often use this scam to trick you into divulging personal data