

Debit Card Fraud Alerts via Mobile **Frequently Asked Questions**

Why should I enroll in Mobile Card Fraud Alerts?

We monitor transactions that appear on your card for potential fraud. When we identify a transaction that may be fraudulent, we may block that transaction and further use of your card until we receive confirmation from you that the requested transaction was legitimate. Mobile Card Fraud Alerts establishes faster communication between you and us so that we may un-block your card more quickly.

How do I register?

If you have a valid mobile number on file, you will automatically receive an enrollment text. If you initially opted-out of receiving alerts and wish to enroll, you can follow these simple steps.

1. Visit <https://www.mercbank.com/>, visit the Personal or Business Card Services Page and the "Enroll in Text Fraud Alerts" tab.
2. Enter the requested information
3. Click "Submit"

Upon "Submit", a message will display telling you to expect a text message from 20733 (this is the only number you will receive fraud text alerts from for us). Reply "Yes" to the text message within 72 hours to complete your enrollment.

You can also visit your local branch or call 800-453-8700 to request this service.

******Please note, you will receive an enrollment message for each active debit card you have on file with us that has a valid cell phone number.******

How much does it cost to use this service?

The Bank does not charge for this service; however, standard text and data rates assessed by your carrier may apply.

How long should it take to receive a text message (SMS)?

Typically, alerts arrive within a few minutes but timing may vary based on your mobile provider and accessibility to your mobile network. If a charge occurs before 8am or after 9pm, you will not receive a text until within that timeframe. In some cases, your card may be blocked from further transactions until we are able to contact you. You can reach us by calling 800-453-8700.

Why did I not receive a fraud alert and my card was blocked when I made a purchase late at night?

The hours we will contact you are 8am to 9pm. This timeframe is based on the time zone of your mobile device area code. If a charge that we suspect may be fraudulent occurs outside of that timeframe, we will not send you a text until within the timeframe.

What if I don't have text messaging?

Text messaging is required for this service. If your mobile phone is able to send and receive text messages, but you do not currently subscribe to a text messaging service, you will need to contact your mobile phone provider to add the text messaging feature to your mobile phone plan.

If I am traveling outside of the U.S., can I receive text message alerts?

Yes. As long as international usage is activated on your mobile device and you are in an area where connectivity is strong enough to receive the text.

It is always a good idea to inform us of your travel plans by calling 800-453-8700 prior to traveling. Doing so will help avoid legitimate charges being flagged as potentially fraudulent.

Can I add multiple phone numbers?

No. You can only link one mobile number per card.

If my mobile phone number changes, what do I need to do?

You will need to contact the Bank to request an update to your mobile phone on record. A new enrollment message will then be sent to the updated mobile phone number.

Do I have to text personal information?

We will never ask you to text us personal information, such as account number, birth date, social security number, mother's maiden name or address. If you ever receive a text message asking for these types of information, please do not respond and contact us at 800-453-8700.

How do I unsubscribe from this service?

Send a text that says "Stop" to 20733 or reply "Stop" to any fraud alert message you receive. This will cancel any further alerts for the card number associated with the text you received. You will receive an opt-out confirmation.

What makes a transaction appear suspicious and generate a Mobile Card Fraud Alert?

Our fraud alert service encompasses multiple strategies driven by current fraud trends. We look at many variable when determining that a transaction is suspicious and potentially fraudulent (for example, the number, dollar amount and rate of transactions, merchant type and location).

We also monitor prior account usage patterns, for example a transaction that is presented from a geographical location not consistent with your other account transactions.

In some cases, the characteristics of multiple transactions may raise suspicion. The text message you receive may ask about more than one transaction.

Will you continue to call me when a suspicious transaction appears on my account?

Yes. If we do not receive a reply text back from you, we will call you at the phone number we have on file during our customer service hours of 8am-9pm.

What if my registered card had fraud?

If you confirm that your card has had a fraudulent transaction, the card will be closed and a new card ordered. You will receive an enrollment text for the new card.