Fraud Alerts FAQ

1. **What are fraud alerts?**

   Fraud alerts are automated phone calls, text messages and emails that are sent when potentially fraudulent purchase activity has been detected on a credit/debit card account. Messages are triggered by the Merck Sharp and Dohme FCU fraud detection system.

   Text messages will be sent to cardholders in the 50 United States at no charge.

   Customers with international telephone numbers will only receive emails. They will not receive text messages or phone calls.

2. **Why am I receiving a fraud alert?**

   Fraud alerts are sent to cardholders when potentially fraudulent transactions are detected on their accounts. We want to ensure that any questionable transactions were authorized by the cardholder.

3. **Will fraud alerts contain any personal information?**

   We will not transmit sensitive personal information through alerts.

4. **Will I get fraud alerts while I am traveling domestically/internationally?**

   If you are travelling within the U.S., you will receive phone calls, text messages and emails. If you are travelling internationally, you will receive emails. You will only receive text messages if your mobile phone plan allows you to receive them while traveling outside of the United States.

5. **What phone number(s) will receive fraud alerts?**

   Any phone numbers that Merck Sharp and Dohme FCU has in your records may be sent alerts.

6. **How do I update my contact information (phone numbers, email addresses, etc.)?**

   1. **Visit** a local branch.
   2. **Email** info@msdfcu.org with an Account Change Form and Photo ID.
   3. **Desktop Online Banking**. Click on>Profile image>Settings>Contact tab- and update your account information.
   4. **Mobile App** Click on> More …>Setting> Contact and update your account information.

7. How do I stop receiving fraud alerts? What should I do if I don't want to get a fraud alert at a certain phone number?

1. You can opt out of text alerts by replying "STOP" to the text message
2. You can opt out of phone calls when the alert system calls you.
3. Click on the Unsubscribe link in the email to stop the emails.
4. Contact our Call Center to ask to stop receiving fraud alerts.
5. Visit a branch to ask to stop receiving fraud alerts.

8. I accidentally opted out of receiving fraud alerts. How do I opt back in?

If you accidentally opted of out text alerts from a mobile phone, when the digital system calls to verify activity, the system will provide the opportunity to opt back into text alerts for the mobile phone. For all fraud alert types, please call the number on the back of your card to re-enable fraud alerts to an email address, a mobile phone or landline phone number. You can also visit a branch for assistance.

9. I have a joint credit card with another cardholder. Why did I not receive a fraud alert? (Or: Why am I receiving fraud alerts when someone else on my account is making a transaction?)

Fraud Alerts are transmitted to the phone number(s) and/or email address associated with the card used at the time of the transaction. If a joint cardholder is receiving alerts, it is because that cardholder's phone number and/or email address is associated with the card transacting. If the fraud alerts should have gone to another cardholder on your account, we ask that you update the contact information for that cardholder.

10. A legitimate transaction triggered a fraud alert. How long should I wait after responding to an alert to reattempt the transaction?

Upon confirming that a transaction is valid, you may retry the transaction immediately.

11. I accidentally marked a valid transaction as fraudulent. What do I do now?

When you mark a transaction as fraudulent, the response message you receive will include our fraud detection department's toll-free number and it asks that you call to review the card activity, or you will receive a call from a fraud detection agent to review. The agent will be able to review the activity with you and clear the card for use.

12. I accidentally responded to an alert that a fraudulent transaction was valid. What do I do now?

Please report the unauthorized transaction immediately by calling the phone number provided in the alerts or the number on the back of your card. The agent will then take care of marking the transaction as fraud and close the card.

13. Will I be responsible for paying for the fraudulent charges?

Please monitor your transactions regularly and review your statements very carefully and immediately report any fraudulent activity to us. Responsibility may depend on the type of card you have and should be verified with us immediately.

14. What should I do if I lose my cell phone and/or obtain a new cell number?

We recommend that you contact your wireless service provider if you lose your phone. If you plan to change your cell phone number, please refer to question number 6 above for help in updating your contact information.

15. What happens if I did not reply to a fraud alert whether via Email, Text or Phone?

Your card may be blocked for use and future transactions would be declined until the fraud alert is cleared.

16. What phone number should I call if I do not have record of being alerted of suspected fraud and thus do not have the call back phone number?

You may call our Customer Service phone number on the back of your card.

17. Do I need to sign up to receive fraud alerts?

You will automatically be enrolled to receive all fraud alerts via the contact methods on your account, ie., email address, cell phone, home phone, work phone, etc.

18. What if I do not have an email, cell or landline phone number?

Your account may be blocked due to the potentially fraudulent activity. You may call or visit your financial institution’s branch to review your account activity. It is recommended to have at least one way to be contacted via the fraud alerts system to allow us to reach you quickly to review suspect activity and keep your card available for use.

19. Are the text commands case-sensitive?

No. Commands can be sent as upper-case, lower-case or a mixture of both.

20. What if my card is lost or stolen?

If your card is lost or stolen, when you are issued a new number, your card account is automatically updated, and you automatically retain the ability to continue receiving fraud alerts.

21. Is this service safe and secure?

Yes. Our priority is to protect your personal information. When you return a fraud alert message, we will ask for the unique case # to your specific fraud alert.

22. During what timeframe will the fraud alert calls occur to cardholders?

Call times follow the TCPA (Telephone Consumer Protection Act) rule of not occurring before 8 am and not after 9 pm in the cardholder's respective time zone.