Fraud Resource Guide

FRAUD RESOURCE NUMBERS

FRAUD CENTER PHONE #	FRAUD CENTER TEXT #
800-237-8990 Will show up as an ***incoming call*** from the Fraud Center.	**96923** 2-Way Connect; Fraud Center text messages are ***sent*** from this number

TO CONFIRM FRAUD	LOST/ STOLEN CARDS
855-293-2456 Number is given to members once they have confirmed fraud via text/email.	**888-297-3416** Members can use 24/7 to report a lost or stolen card.

Encourage members to save these numbers on their phones. This will eliminate any confusion about whether a notification they received was from Education First or a scammer.

If the member suspects fraud, ask the member what number shows up on the message. This will be a good indicator of whether it is fraud or not.

Note for the member:

Education First will **NEVER** send you a text or place a call asking you to click on the link or reveal your account information or other sensitive information. If you receive one of these fraudulent communications, DO NOT click on the link or reveal any personal or account information. However, members could receive a link through email to confirm a purchase or report it as fraud (please see page 2 of the Cardholder Fraud Alert Messaging Guide).

Resource Links:

Cardholder Fraud Alert Messaging Guide

Card Services Quick Assist Guide

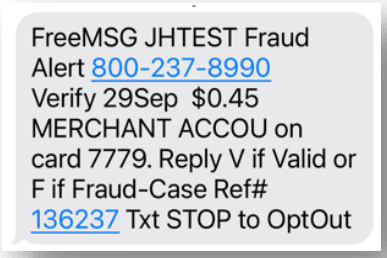
MEMBER IDENTITY CONFIRMATION:

Effective November 1, 2023

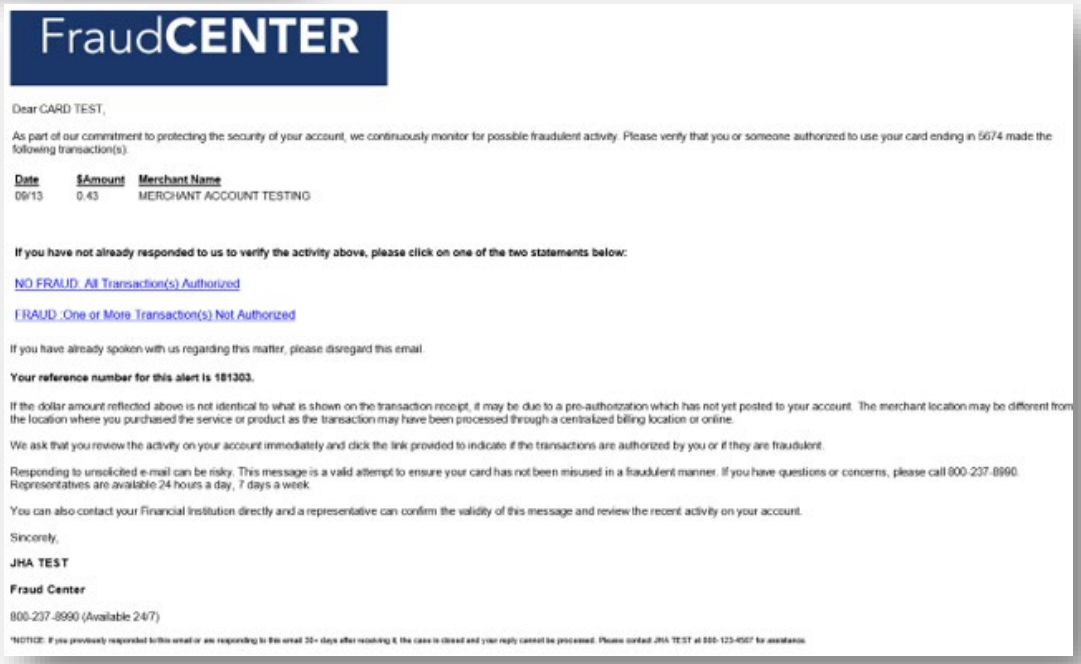
Members will be given a **6-digit reference number** via outbound SMS, email, or voicemail.

Cardholders will be required to provide their case reference number to authenticate themselves in inbound calls to the IVR or our live agents in the call center.

SMS TEXT:



Email Example:



FraudCENTER

Dear CARD TEST,

As part of our commitment to protecting the security of your account, we continuously monitor for possible fraudulent activity. Please verify that you or someone authorized to use your card ending in 5674 made the following transaction(s).

Date	$Amount	Merchant Name
09/13	0.43	MERCHANT ACCOUNT TESTING

If you have not already responded to us to verify the activity above, please click on one of the two statements below:

NO FRAUD: All Transaction(s) Authorized

FRAUD :One or More Transaction(s) Not Authorized

If you have already spoken with us regarding this matter, please disregard this email.

Your reference number for this alert is 181303.

If the dollar amount reflected above is not identical to what is shown on the transaction receipt, it may be due to a pre-authorization which has not yet posted to your account. The merchant location may be different from the location where you purchased the service or product as the transaction may have been processed through a centralized billing location or online.

We ask that you review the activity on your account immediately and click the link provided to indicate if the transactions are authorized by you or if they are fraudulent.

Responding to unsolicited e-mail can be risky. This message is a valid attempt to ensure your card has not been misused in a fraudulent manner. If you have questions or concerns, please call 800-237-8990. Representatives are available 24 hours a day, 7 days a week.

You can also contact your Financial Institution directly and a representative can confirm the validity of this message and review the recent activity on your account.

Sincerely,

JHA TEST

Fraud Center

800-237-8990 (Available 24/7)

*NOTICE: If you previously responded to this email or are responding to this email 30+ days after receiving it, the case is closed and your reply cannot be processed. Please contact JHA TEST at 800-123-4567 for assistance.

Voicemail Example:

"This is the Fraud Center calling on behalf of Test Bank calling for Test Cardholder. We would like to verify recent activity on your MasterCard ending in 5674. Your card may have a temporary restriction in place. It's important that you call us back at your earliest convenience. We are available 24 hours a day, seven days a week. Please make note your case reference ID to respond to this case is 181303. You will be required to provide this value when you call back at 800-237-8990. Thank you. Goodbye."

The **6-digit case reference number** will be included in the memo posted to QuickAssist for user access as well.

Note: Implementation of this case management fee will result in a $0.05 increase in the Fraud Alert Case Management fee.

This new requirement will provide better security, in hopes of preventing more fraud.

MEMBER NOTIFICATIONS:

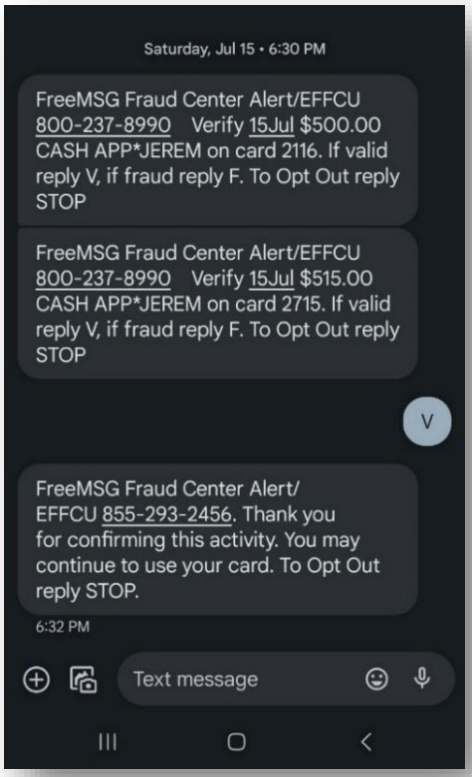
How a member will receive a legitimate notification(s) from Education First FCU

TEXT ALERTS

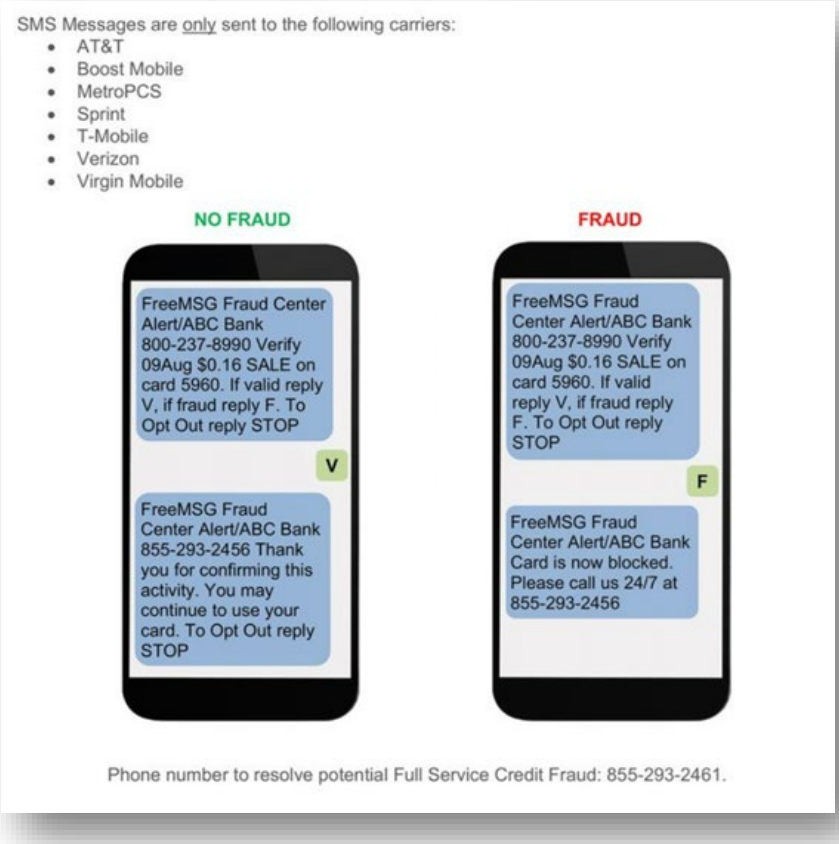
Text Alert for fraud from 96923

When a member receives a text message about **confirming** or **denying** a charge, they will be prompted to enter the letter **V** to verify the charge or the letter **F**, to report the charge as fraud.

Example of this text alert



Another example:

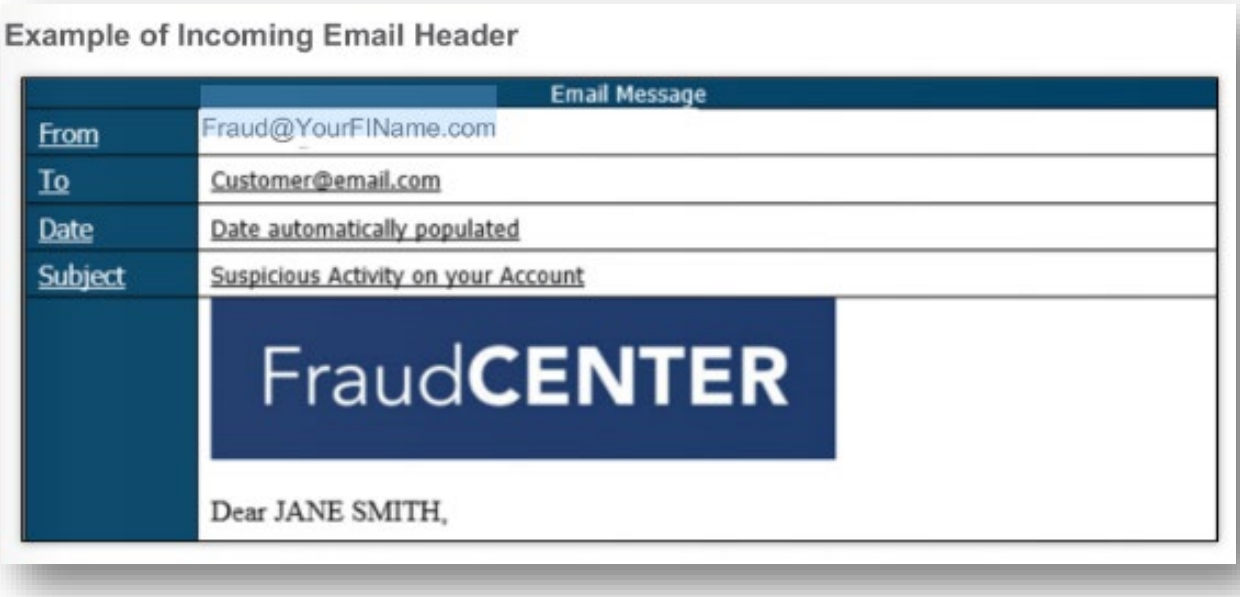


MEMBER NOTIFICATIONS:

How a member will receive a legitimate notification(s) from Education First FCU

EMAIL ALERTS

Email Notification: From **Fraud@educationfirstfcu.org**



FRAUD CENTER PHONE CALLS

Receiving a call from **800-237-8990**

When a transaction is queued, the member will be notified in the following order. If any contact information is missing from any of these fields, the system skips that method and moves on to the next method that is populated.

1. **Text Message:** Immediately after alert
2. **Email:** Within 5 minutes
3. **Home Voice Call:** Within 5 minutes
4. **Cell Voice Call:** Within 8 hours
5. **Work Voice Call:** End

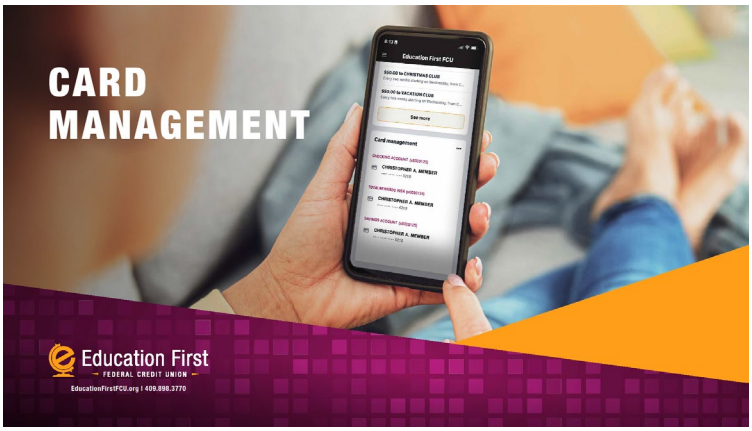
MEMBER TOOLS

Card Management Tools in Online Banking

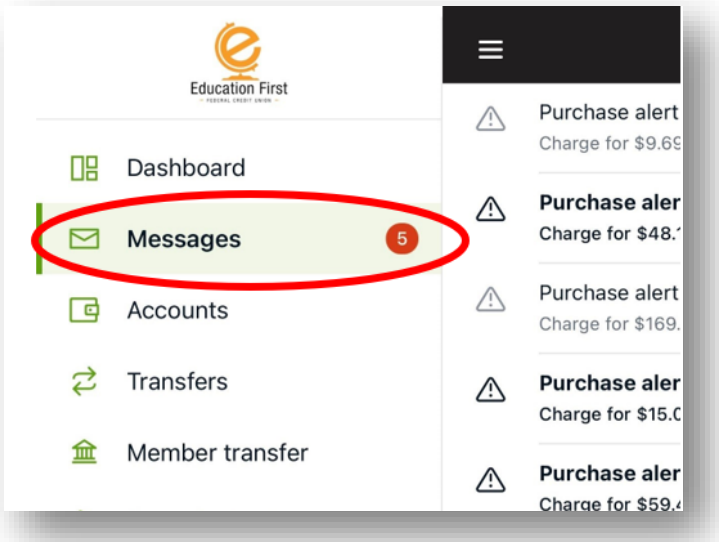
Purchase Alerts

For purchase and transaction alerts, the member will receive alerts through their Online Banking Account, **IF** alerts for purchases and transactions have been turned on by the user.

If the member does not have these alerts turned on, you can send them a step-by-step tutorial on how it can be done, by double-clicking the picture below.



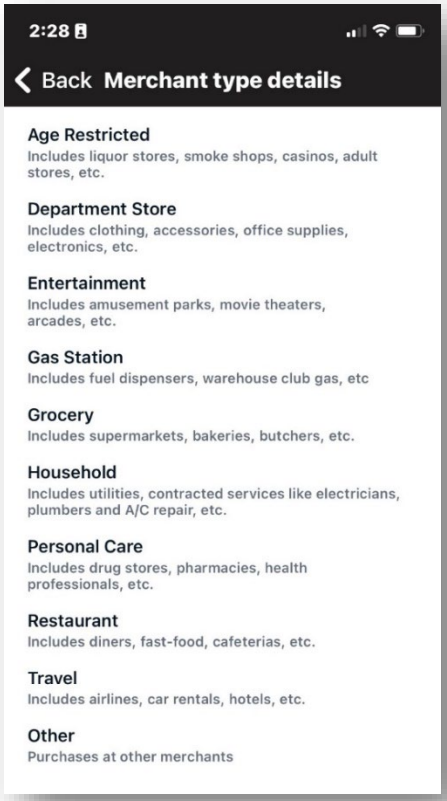
Once Purchase Alerts are turned on, this is how notifications will show up within online banking:

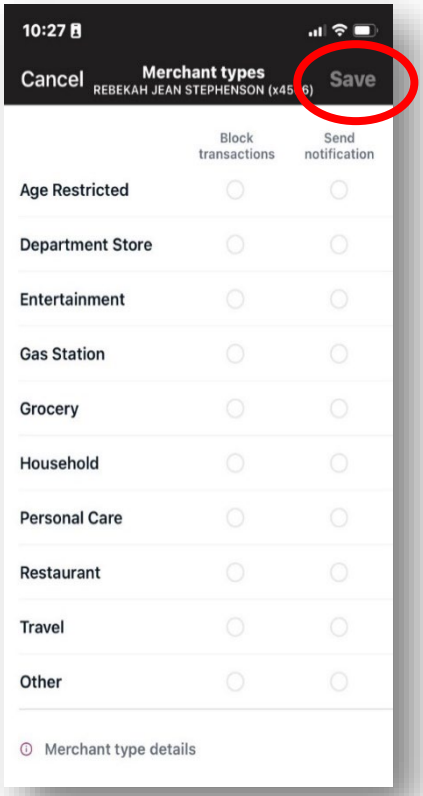


MEMBER TOOLS

Alert/Block based on Merchant Types

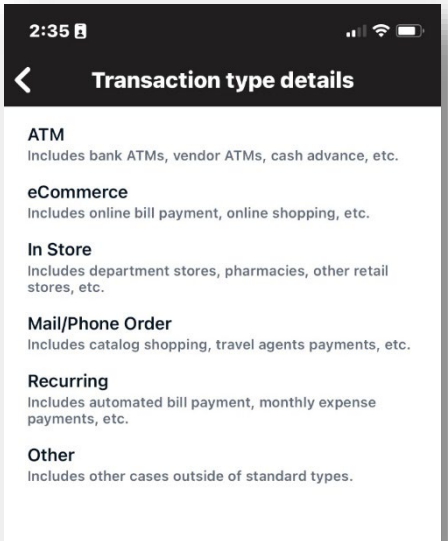
- These alerts are based on the type of merchant where the transaction occurred.
- The member may select to block the transactions and/or receive notifications.
- They can make their selections and then hit save.

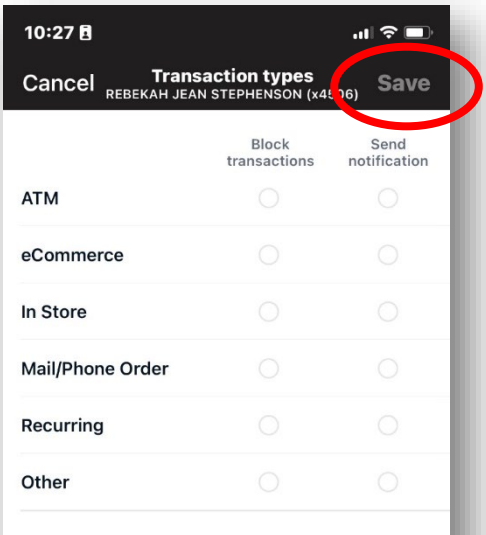




Alert/Block based on Transaction Types

- These alerts are based on the type of transaction at the point of sale.
- The member may select to block the transactions and/or receive notifications.
- They can make their selections and then hit save.





MEMBER TOOLS

Alert/Block Transaction single/monthly spending limits

- These alerts are based on the threshold amount set by the member.
- The member can either restrict a transaction based on the dollar amount per transaction or based on a monthly limit.
- They can set their limits and click save.