What to Know About FFB Debit Card Fraud Alerts

- A text alert from us warning of suspicious activity on your card will NEVER include a link to be clicked. Never click on a link in a text message that is supposedly from us. A valid notification will provide information about the suspect transaction and ask the cardholder to reply to the text message with answers such as 'yes', 'no', 'help', or 'stop'. It will never include a link.

- A text alert from us will always be from a 5-digit number and NOT a 10-digit number resembling a phone number. Text caller IDs will be 37268.

- A phone call from our institution's automated dialer will only include a request for your zip code, and no other personal information, unless you confirm that a transaction is fraudulent. Only then will you be transferred to an agent who will ask questions to confirm that you are the actual cardholder before going through your transactions with you. If at any point you are uncertain about questions being asked or the call itself, hang up and call us directly. If a call is received by the cardholder, claiming to be our call center and asking to verify transactions, no information should have to be provided by the cardholder other than their zip code, and a 'yes' or 'no' to the transaction provided.

- If you ever receive a request for personal information that claims to be from us, have questions regarding scams, or need help with other concerns, contact us at 1-800-562-6896 and ask for our Electronic Banking Department or email us at abuse@ffb1.com.

- We will NEVER ask you for your PIN or the 3-digit security code on the back of your card. Don't give them out to anyone, no matter what they say. Hang up and call us directly. Fraudsters will often ask cardholders to verify fake transactions. When the cardholder says no, they did not perform those transactions, the fraudster then says that their card will be blocked, a new card will be issued, and that they need the card's PIN to put it on the new card. Many people believe this and provide their PIN. The 3-digit CV2 code on the back of the card will allow a fraudster to conduct transactions.

- Regularly check your account online to see if there are any suspicious transactions that have occurred, but especially if you are unsure about a call.