Cardholder Fraud Education

During this busy time of year, we want to remind you how stolen cardholder information is used to commit fraud. Fraudsters will attempt to have you share information they need to commit fraud by posing as a financial institution call center, or by sending text messages that look like they are coming from your financial institution, warning of suspicious transaction activities.

Below are helpful tips to avoid compromising your personal information:

• Text alerts warning you of suspicious activity on your card will NEVER include a link to be clicked. Cardholders should never click on a link in a text message that is supposedly from your financial institution. A valid notification will provide information about the suspected transaction and ask you to reply to the text message with answers such as 'yes', 'no', 'help', or 'stop,' and will never include a link.

• A text alert will always be from a 5-digit number and NOT a 10-digit number resembling a phone number.

• A phone call from Fraud Department (automated dialer) will only include a request for your Zip code, and no other personal information, unless they confirm that a transaction is fraudulent. Only then will you be transferred to an agent who will ask questions to confirm your identity before going through the transactions. If at any point you are uncertain about questions being asked or the call itself, please hang up and call the financial institution directly. If you receive a call claiming to be the Fraud Department call center asking to verify transactions, no information should have to be provided by you other than Zip code and a 'yes' or 'no' to the transaction provided.

• The Fraud Department will NEVER ask for the PIN or the 3-digit security code on the back of a card.

• Posing as Fraud Department call center agents, fraudsters will often ask you to verify fake transactions. When you say no, you did not perform those transactions, the fraudster then says that your card will be blocked, a new card will be issued, and that they need the card's PIN to put on the new card. Many people believe this and provide their PIN. DO NOT provide you PIN or any other password information!

• Please regularly check your account(s) online for suspicious transactions, but especially if you are unsure about a call or text message you've received. If anything looks amiss, please call the financial institution directly for assistance.

• If you have received a voice or a text message from fraud department call center and are unsure about responding to it, please call you financial institution directly for assistance.

If you wish to learn about additional fraud prevention tools such as CardValet, please contact us 281-449-0109.