Information on Cardholder Fraud Attempts

D.L. Evans Bank has been made aware of a fraud attempt that may be seen by our customers. These fraudsters are pretending to be from Fiserv, which is a product used by D.L. Evans Bank for debit cards. We wanted to make sure that our cardholders are aware of the scam and can use the following information to protect themselves.

Below are a few tips to help you avoid compromising your personal information:

1. Text messages that alert cardholders of warning of suspicious activity on their card will NEVER include a link to be clicked on. Cardholders should never click on a link in a text message that is supposedly from Fiserv. A valid notification from Fiserv will provide information about the suspect transaction and will only ask the cardholder to reply to the text message with answers such as 'yes', 'no', 'help', or 'stop'.
2. A text alert will always be from a 5-digit number and NOT a 10-digit number resembling a phone number. Text caller IDs for legitimate messages from Fiserv will be either 20733 or 37268.
3. If at any point you are uncertain about questions being asked or the call itself, please hang-up and call your local D.L. Evans Bank branch.
4. If you receive a call claiming to be the Fiserv call center asking you to verify transactions, the only information that should be provided by you (the cardholder) should be your zip code and "yes" or "no" responses, unless you 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 your transactions.
5. Fiserv will NEVER ask for the PIN or 3-digit security code on the back of a card.
6. Posing as call center agents, fraudsters will often ask cardholders to verify fake transactions. When the cardholder says no, they did not perform those transactions, the fraudster then says their card will be blocked, a new card will be issued, and that they need the card's PIN to put on the new card. Hang up immediately and do NOT give them your PIN.
7. We advise that you regularly check your account(s) online for suspicious transactions, but especially if you are unsure about a call or text message you have received. If anything looks wrong give your local branch a call. We would rather have you call and let us confirm nothing is wrong than have you be a victim of cardholder fraud.

Your local branch is a great resource for making sure you avoid fraudsters. If you are ever in doubt of a phone call or text message, please call or visit your local branch to review transactions or confirm activity on your card. You can also utilize our D.L. Evans mobile banking app or CardValet services to temporarily deactivate your card until you can confirm the information has not been stolen.