

TO: Denison State Bank account holders:

March 1, 2024

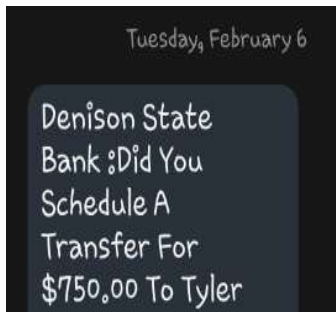
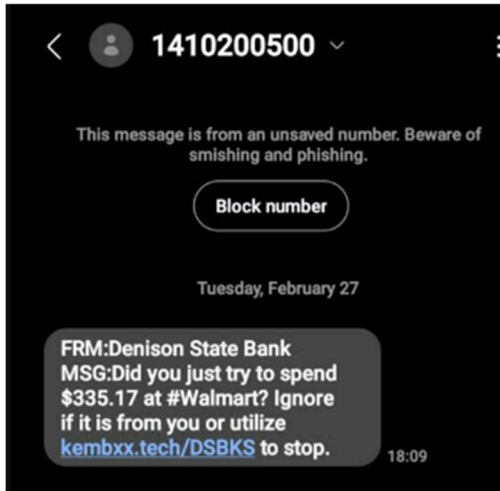
**To avoid ongoing bank scams and fraud, read on:**

Fraudsters and scammers continue to impersonate banks and contact account holders to steal their money. Denison State Bank is informing customers here about what is a legitimate communication from the bank and what is not.

At the bottom of this message is a re-posting from June 2023 to all our customers about what are the legitimate ways that DSB communicates with account holders. Next, though, we re-emphasize these very 4 important facts:

**1). SUSPICIOUS DEBIT CARD ACTIVITY: NO, Denison State Bank does not send texts and emails to card holders about suspicious card activity.** The only way that DSB or our card monitoring agency *Card Sentry* contacts card holders is through live-person phone calls. See example here of fraudulent texts that have been reported.

**Examples of fraud texts:**



3176076950

Denison State Bank:

We noticed an unusual activity on your ACCOUNT with us. A temporary hold has been placed, you are required to VISIT below to regain access now.

<http://tinyurl.com/denisonstatebk>

(continued on next page)

**2). TEXT ALERTS: NO,** Denison State Bank does not send texts about suspicious account postings, demanding immediate action. The only text alerts we issue are the ones that account holders create in their DSBconnect digital banking “Manage Alerts,” “Manage Cards,” and “Statements and Notices.”

**3). DSBconnect LOGIN PASSWORD: NO,** Denison State Bank will never ask you for your DSBconnect password. Even here in our bank systems, we cannot see the actual passwords that customers use.

**4). CARDS and DIGITAL NOT RELATED. NO,** Denison State Bank will never ask you for your DSBconnect login credentials in order to address situations on your debit card or account postings. While phone numbers, texts and email addresses are now being used as multi-factor authentications in order to login to DSBconnect, we do not ask questions about your digital banking in order to address and fix situations on debit cards.

We ask that all account holders be very discerning about communications you receive that claim to be from Denison State Bank. Read the following guide and refer to the information on our bank web site. If you are ever in doubt, do not respond and check with the bank first. If any question, feel free to respond back here or at [online@dsbks.com](mailto:online@dsbks.com).

Sincerely,

**Denison State Bank, Digital Banking**

---








**Re-posted: March 2024**

**TO: All DSBconnect users at Denison State Bank:**

The following table shows the methods that Denison State Bank and its contracted vendors use to communicate with account holders and cardholders. Details on each follow:

*(continued next page)*

**DENISON STATE BANK: How we communicate with account holders**

Activity Type	Communication Sender:	Communication Method:	When:
Suspicious DEBIT card activity detected	CSI Card Sentry	 Live-agent phone call; no text or email.	8:00 a.m. to 9:00 p.m. CST. Return calls can be made by cardholders to CSI Card Sentry 24/7.
Suspicious DEBIT card activity detected	DSB employees	 Phone call or email ending in "@dsbks.com"	7:00 a.m. to 6:30 p.m. weekdays, possible on weekends, as detected by any employee.
Suspicious account activity detected	DSB employees	 Phone call or email ending in "@dsbks.com"	7:00 a.m. to 6:30 p.m. weekdays, possible on weekends, as detected by any employee.
DSBconnect digital banking alerts	System-generated	 Text or email alerts as only set up by the registered account holder.	As set by the customer user.
DSB Visa DEBIT card usage alerts	System-generated	 Text or email alerts as only set up or requested by the cardholder.	Within seconds any time a card number is approved or declined.
Confirmation of mobile check deposit receipt and status	System-generated	 Two emails are sent: the first when the bank receives the mobile deposited item; the second when the item is processed showing approval or decline status. Similar emails may be sent on the Business desktop check deposit system.	8:00 a.m. to 6:00 p.m. CST, only weekdays. Mobile check deposits are not received or processed on Saturdays, Sundays and closed holidays.
Online statements & notices issued	System-generated	 Sent to the email address on file at the bank that notifies of the issuance of a registered online statement or online notice, for DSBconnect digital banking and CSISafe.	Any time our systems generate these registered statements and notices.

*(continued next page)*

**Suspicious DEBIT card activity: *Phone call:*** DSB contracts with “CSI Card Sentry” to monitor for suspicious activity 24/7 on the Visa debit cards issued by DSB. If suspicious activity is detected, a live agent at Card Sentry will: 1) attempt to call the cardholder from 8:00 a.m. to 9:00 p.m. any day of week to the phone number on file at the bank and verify with the cardholder if the activity was authorized or not; if unauthorized, or card lost or stolen, Card Sentry will put the card on Restricted status so that it cannot be used; if unable to make contact, the agent will leave a voicemail if possible; and 2) Card Sentry will email the bank with what was detected and what, if any, was verified, and the bank will see that the next morning and contact the cardholder with additional recovery steps if needed.

Card Sentry live agents contact cardholders by phone only and not by texts or emails. The agent will only ask if the activity is authorized or not; the agent will never ask for card number, card PIN or digital banking login credentials.

There may be times when bank employees who work on card fraud may send emails to impacted cardholders from their bank email ending in “@dsbks.com” and/or by phone calls to cardholders, and they will always identify themselves as being with Denison State Bank.

**Suspicious account activity: *Phone call or email:*** The only other communications with account holders about suspicious activity will come directly from bank employees working at the main office and/or branches of Denison State Bank. They will make phone calls or emails that end in “@dsbks.com”. This can be for suspicious activity on account postings, incoming and outgoing electronic transactions and transfers, check clearings and the like.

**DSBconnect alerts: *Text or email:*** Registered users of DSBconnect digital banking can set up their own account and transaction alerts. There are Custom alerts, Bill Pay alerts and Security alerts that can be set up for various triggering situations. Users select email and/or text messages. Set this up within DSBconnect > Documents & Alerts > Manage Alerts.

**Debit card usage alerts: *Text or email:*** DSB Visa debit cardholders can set up usage alerts that are sent when their card number is approved or declined. The alert only reports the approval or decline status; it does not detect suspicious activity or ask for verification. Set this up within DSBconnect > Documents & Alerts > Manage Cards.

**Mobile check deposits: *Email:*** when a DSBconnect app user captures and submits an image of a check item for deposit into their bank account, a confirmation email is sent to the email address on file once the bank receives the item, and a second email is sent once

the item is processed, showing approval or decline status (and reason why). Make remote mobile deposits within DSBconnect > Transfer Money > Mobile Check Deposit.

**Online statements and notices:** *Email:* when an account that is registered for statements and notices via DSBconnect or CSISafe generates a statement/notice, an email notice is sent to the email address on file. The statement/notice PDF file is not contained in the email message. Register for online statements within DSBconnect > Documents & Alerts > Statements & Notices.

**DSBconnect mass messages:** *Posted within secure DSBconnect login:* DSB at times will post messages, like this one, to all DSBconnect users or to groups of users. These will display in the Connect > Messages With DBS section in the main menu. These are posted directly with the logins of the users and are not sent on email. The information, in full or in part, may also be posted on the bank's web site [www.dsbks.com](http://www.dsbks.com)

## **DENISON STATE BANK**

**Emails:** all end in "@dsbks.com" Send questions to: [online@dsbks.com](mailto:online@dsbks.com)

**Web:** [www.dsbks.com](http://www.dsbks.com) **Call:** (785) 364-3131