DSBconnect Digital Banking
Out of Band Multi-Factor Authentication (OOBA MFA)

A new required additional identity authentication to help minimize risk of unauthorized logins and access in digital banking

TO: All DSBconnect Digital Banking Users,

Due to an increase in frauds and scams being presented to the banking consumers locally and around the nation, Denison State Bank is increasing the security used for logins to DSBconnect digital banking, starting Dec. 6, 2023.

The next login you make to DSBconnect on or after Dec. 6, 2023, will trigger the set-up of an "Out Of Band" multi-factor authentication (OOBA MFA) profile. Authentication needed for logins, when triggered, will be in the form of a text verification, or an automated phone call verification, or a Duo app verification, all based on information on the device being used by the user. Said simply, when the bank knows that the user identity and device being used belongs to the registered account holder, we can identify situations when the opposite is happening when done by an unauthorized person on an unrecognized device. Adding this additional layer of authentication will minimize the risks of unauthorized logins commonly done in fraud and scam situations that pressure the digital user to reveal their login credentials, and the fraudster can then attempt to login as the user and illegally access and transfer funds out of accounts. This will help ensure that only the registered user is able to login and access their bank account information.

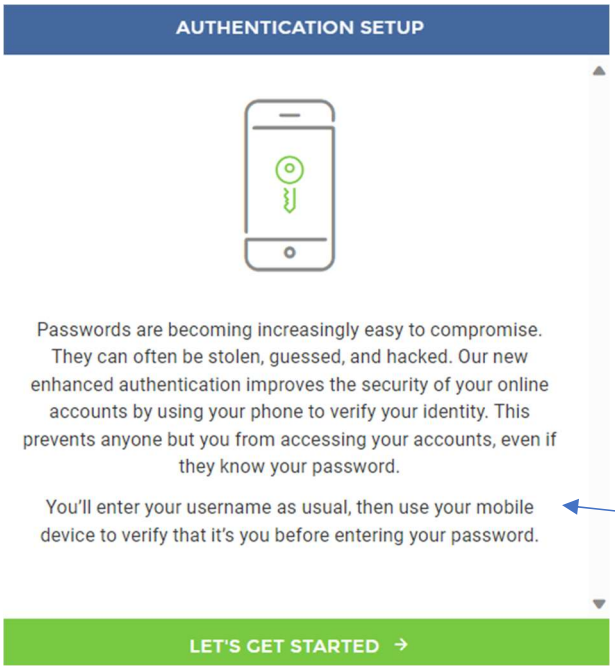
SET-UP: WHAT WILL IT LOOK LIKE:

To establish this, at your first DSBconnect login, either on bank web site or bank mobile app on or after Nov. xx, you will be prompted to follow and fill in the fields on the screens to set-up your OOBA MFA.

(Note: some of the language used on these set-up screens is outdated, as noted).

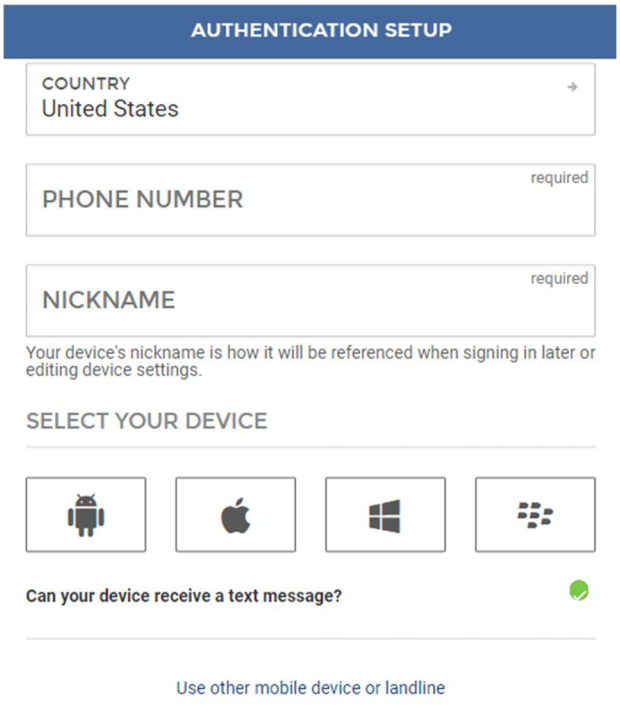
Click the "Let's Get Started" green bar:

(continued on next pages)



UPDATE: After you login with username-password combo, or with Thumbprint or Eye scan, if triggered, you will be prompted for the OOBA MFA.

Next screen:



COUNTRY: Keep country as "United States" unless different.

PHONE NUMBER: Key in your 10-digit mobile phone number to use for authentication. If you prefer to use a landline or another device not being used now during this set-up, at bottom, first click the "Use other mobile device or landline."

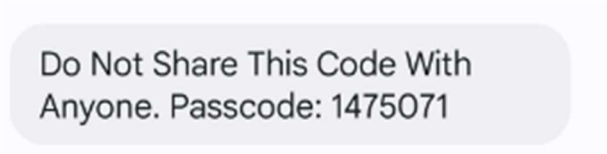
NICKNAME: Nickname it however you want it to display to you.

SELECT DEVICE: Click the type of mobile phone you use from the logo choices shown.

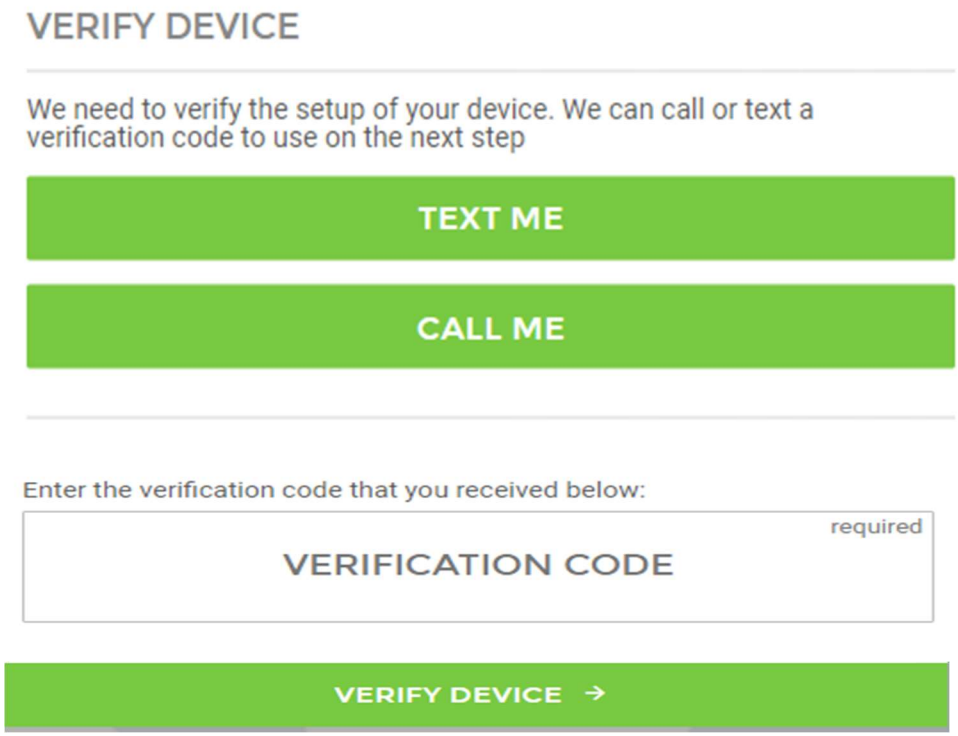
RECEIVE TEXT MESSAGE?: The default setting is Yes; if not able, click it off.

VERIFY DEVICE: click "Text Me" or "Call Me", whichever you prefer, for the first-time verification.

If text: the sending text number will be "386732". Obtain the one-time verification code that was just texted to you (see example here) and key it in on the app box "Verification," then "Verify Device."



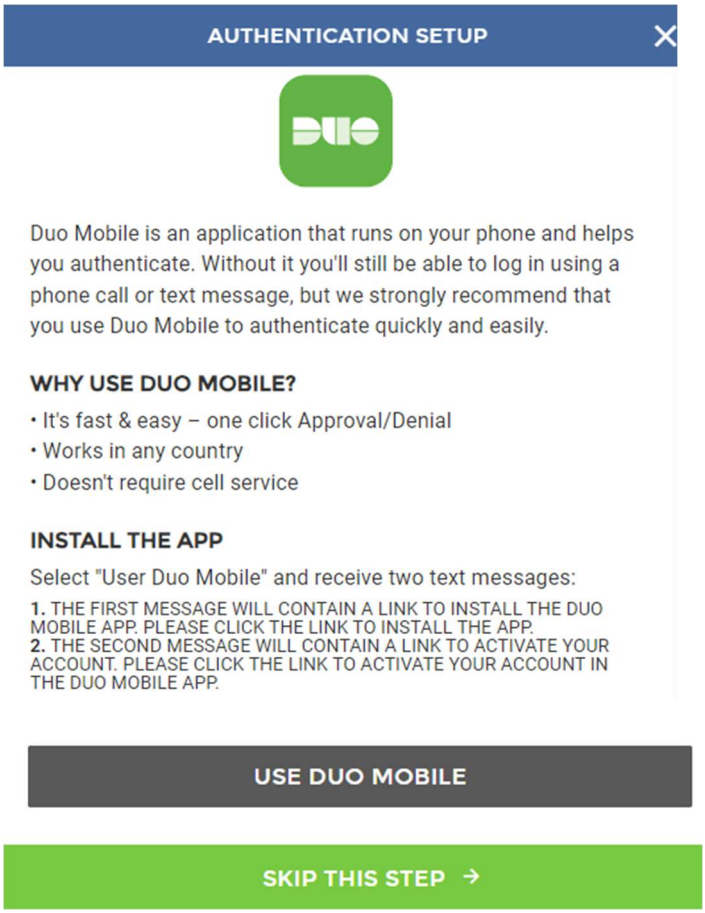
If phone: the calling number will be "Denison State Bank (785) 364-3131". The automated voice will announce a one-time verification code to you to key in on the app, then "Verify Device."



TO AVOID FRAUD: Never reveal this verification code to anyone else. There never will be a reason for the bank, nor any other person, to ask you for the code.

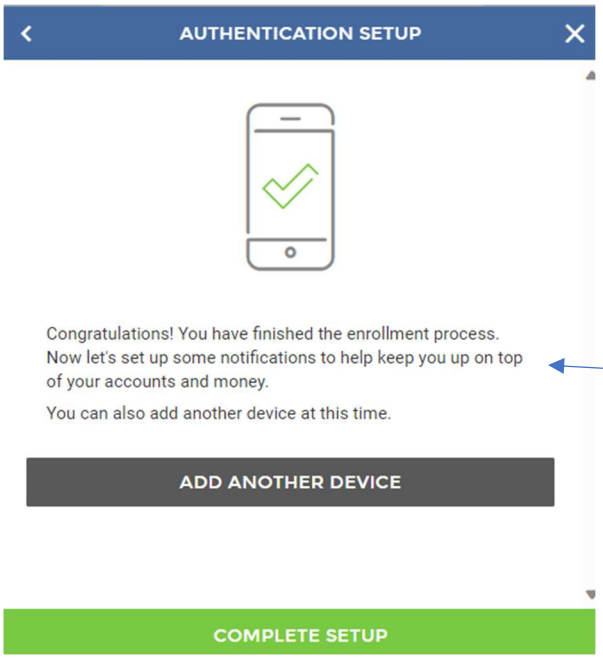
Next screen:

The Duo Mobile app will be presented as an optional way to verify. You are not required to use Duo, and if not interested, click "Skip This Step." If interested in using, click "Use Duo Mobile". A link to install the Duo app will be immediately texted to your mobile phone number from Duo sender number 68874. Click to activate and/or install the app, even if you already have Duo installed on your phone, in order to complete. When Duo is prompted for future logins, follow the Duo screens to use. (Note: Denison State Bank is not affiliated with Duo and does not provide end-user support on using Duo).



If you have another mobile phone device you want to register for authentications, click "Add Another Device. If not, click "Complete Setup."

Next screen:



UPDATED: Notifications set-up is not prompted here. You can skip this and go to "Complete Setup"

AFTER SET-UP

HOW YOUR DEVICE IS RECOGNIZED:

Our system remembers user devices by recording a "Device Fingerprint." Specific information from the user's browser on that device is recorded to create a unique device fingerprint that is then logged if the user marks the "Remember this device" checkbox on the security question screen of the login process. The system will identify any new device and will remember the device until the device reaches its expiration date or if the user clear off their identifying information. Users will not be prompted with the OOBA or MFA security question when logging in from a device that has been identified and has not expired.

WHEN OOBA MFA GETS TRIGGERED

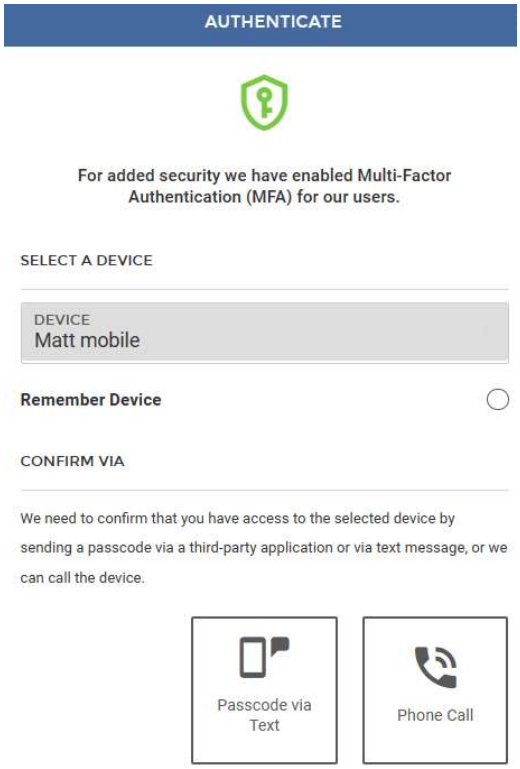
Once your OOBA MFA set-up is complete, the OOBA MFA is triggered based on these factors:

Keep using same recognized device: On your DSBconnect login screen, you are asked if you want to "Remember this device". As long as the device is remembered and recognized through the information already recorded, DSBconnect will not ask for repeated OOBA MFA verification.

Login from a different device: If you login from a different device than the one you set-up the OOBA MFA on, it will not be recognized with your login, and the OOBA MFA will be triggered.

Same device, but un-recognized: If you make certain actions on your device settings, such as "clear the cache" and "clear off cookies," that will make your device un-recognized and un-remembered and will trigger the OOBA MFA verification at next login. Certain anti-virus programs installed on your device may clear and clean identifying information too.

Annual renewal: The device fingerprint we record about your device stays on record for one year. Every 365 days, if not done already, an OOBA MFA will be triggered.



Remember:

Any time your device or browser is not recognized during the login attempt, the OOB MFA will be triggered for verification. Complete it when prompted by entering the verification code that is texted, called, or performed through Duo.

HOW DOES OOBA MFA DETECT AND PREVENT FRAUD

If a user were to reveal their DSBconnect username, password and security answers to a fraudster or bank impersonator, and if that unauthorized person were to then attempt to login as the user on their own device, the OOBA MFA will be prompted, and they will not be able to get past that since they will be unable to access the mobile phone number of the user or the Duo app installed on the user's phone.

Recommendation: **set up a DSBconnect alert for valid and invalid logins.** Anytime your username (which should be known only to you) gets entered on a login attempt, either legit as you or not legit by a non-authorized person, a notice can be texted or emailed to you. Create this in your DSB login > Manage Alerts > click the plus sign "+" to create a new alert > Security Alert > set up both "Login" for all times of day and set up "Login Error" to be notified if your username is attempted but failed.

Q&A

What if I have problems using OOBA MFA?
Contact the bank weekdays 8:00 to 6:00. Depending on the situation, we probably will clear your OOBA that is on file and have the set-up be triggered at your next login.

Must I use a mobile phone device for OOBA MFA to work?
During the set-up, you can choose if you want to use a landline phone number rather than a mobile phone number for verifications to be called to.

What if I change my phone number?
Login, if possible, and click Profile > Phone Number and enter your new phone number there and delete number no longer used. You will be prompted to verify the phone number. If unable to login due to a phone number not on file, contact the bank.

DENISON STATE BANK

Call: (785) 364-3131
Email: online@dsbks.com
Web: www.dsbks.com