



Online Banking Training

First Time Login Process – Retail/Consumer

End-user will enter
their existing Online
Banking ID/Alias or
12-digit NTID



Username

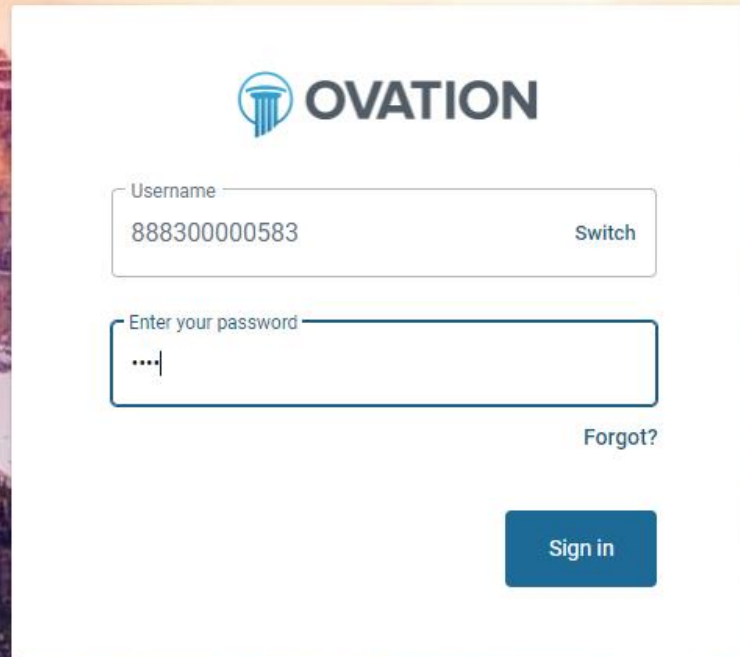
[Forgot?](#)


First time user? Enroll now.

[Continue](#)

 [Open an account](#)

The end-users password will stay in-tact when moving from NetTeller to Banno Online. Passwords will not expire or be required to change.

The image shows a login interface for 'OVATION'. At the top is the logo, which consists of a blue circle containing a stylized classical column, followed by the word 'OVATION' in a bold, black, sans-serif font. Below the logo is a 'Username' label and a text input field containing the number '888300000583'. To the right of the input field is a 'Switch' button. Below the username field is a 'Enter your password' label and a password input field with masked characters '....'. To the right of the password field is a 'Forgot?' link. At the bottom right of the form is a blue 'Sign in' button.

 **OVATION**

Username [Switch](#)

Enter your password [Forgot?](#)

[Sign in](#)



Your password has expired and must be changed.

New password

|

Confirm new password

Show rules

Save

If a customer's password happens to coincidentally expire, or is ever reset, this is what the password change screen looks like on Banno Online



Secure your account

Two-factor authentication adds another layer of security to make sure only you can sign in. Please provide an email and a phone number that you will have access to while signing in to receive a verification code.

Email

spinkley@jackhenry.com

Country

+ 1

US/Canada

Phone

(417) 669-5357

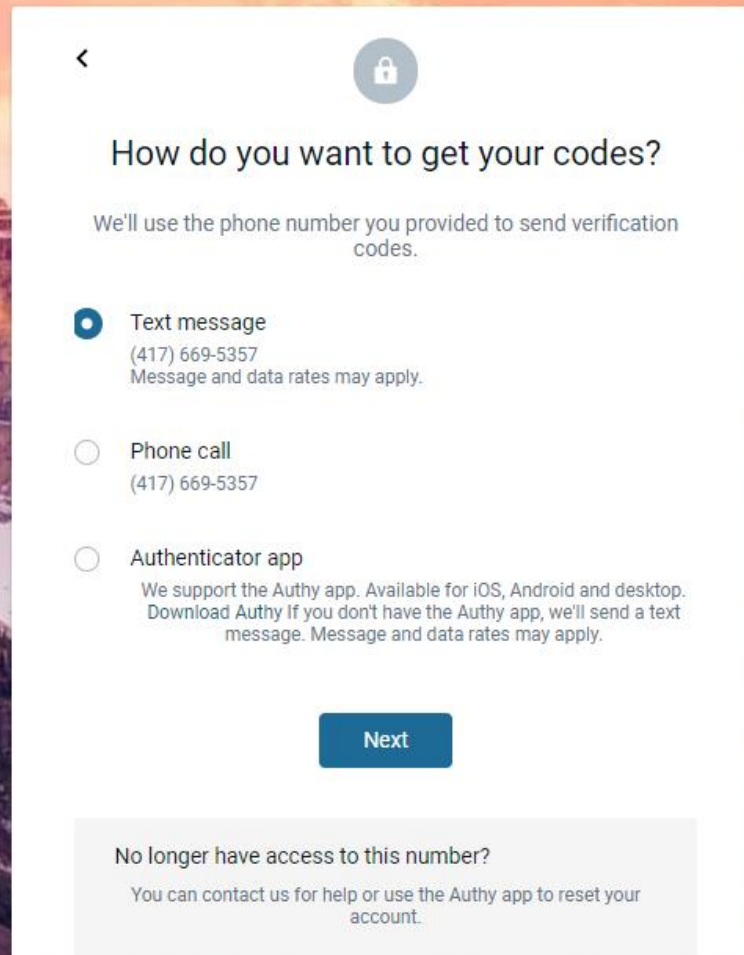
Next

Message and data rates may apply.


Confirm or enter
their email address.

Enter a phone
number that will be
used for 2FA.

Choose the method they want to use to receive their 2FA security code.



The screenshot shows a mobile app interface with a white background. At the top left is a back arrow icon, and at the top right is a lock icon. The main heading is "How do you want to get your codes?". Below this, a subtext reads: "We'll use the phone number you provided to send verification codes." There are three radio button options: "Text message" (selected), "Phone call", and "Authenticator app". Each option includes a phone number "(417) 669-5357" and a note: "Message and data rates may apply." Below the options is a blue "Next" button. At the bottom, there is a light gray box containing the text: "No longer have access to this number? You can contact us for help or use the Authy app to reset your account."

< 

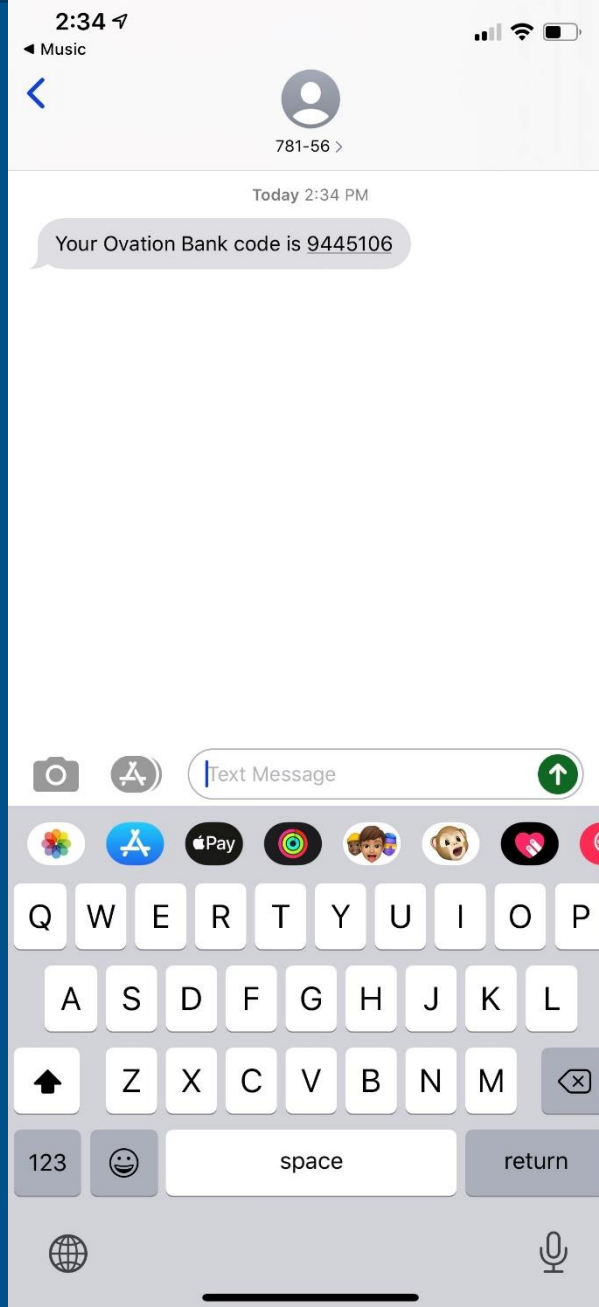
How do you want to get your codes?

We'll use the phone number you provided to send verification codes.


- ☒ Text message
(417) 669-5357
Message and data rates may apply.
- ☐ Phone call
(417) 669-5357
- ☐ Authenticator app
We support the Authy app. Available for iOS, Android and desktop.
Download Authy if you don't have the Authy app, we'll send a text message. Message and data rates may apply.


Next

No longer have access to this number?
You can contact us for help or use the Authy app to reset your account.



Enter the 7-digit security code in the designated field.





Enter verification code

We just sent a text message with a verification code to *****
**57.

Enter code

9445106

☒ Don't ask for codes again on this computer

Verify

Didn't get it?

Resend or Try another way



You're all set!

Two-step verification for your account is now enabled.

Ok

Accept the Online
Banking Terms &
Conditions.



User agreement

TERMS OF USE AND THE PRIVACY POLICY -

The primary licensor for the online and/or mobile banking service you are using (the "Service") is Jack Henry & Associates, Inc. (the "Provider"). By enrolling in our Service, you hereby agree as follows:

(i) General. The Provider is not the provider of any of the financial services available to you through the Service, and the Provider is not responsible for any of the materials, information, products or services made available to you through the Service.

(ii) Provider Privacy Policy. Provider may access personal information while you use the Service. Provider may access records held by your financial institution for such information as your phone number, home address or email address. Provider will use this contact information to alert you about Service-related events or actions that require your attention. If you grant permission to use phone information, Provider will use the phone number to pre-populate forms that expect a personal phone number for contacting. If you grant permission to use your device's location, Provider will use the data when checking for nearby branch and ATM locations. If you grant permission to use access photos, media or other files stored on your device, Provider will use that information to add an image to a transaction and add a photo to your profile. If you grant permission to use a camera, Provider will use it when taking a picture to add an image to a transaction or to capture images of a check that is being deposited or to add a photo to your profile. In addition to this Provider Privacy Policy, your financial institution maintains a privacy policy covering the personal and financial information related to your use of the financial institution's services and products, including such information that may be gathered through use of this Service, such as the "Account

Accept