

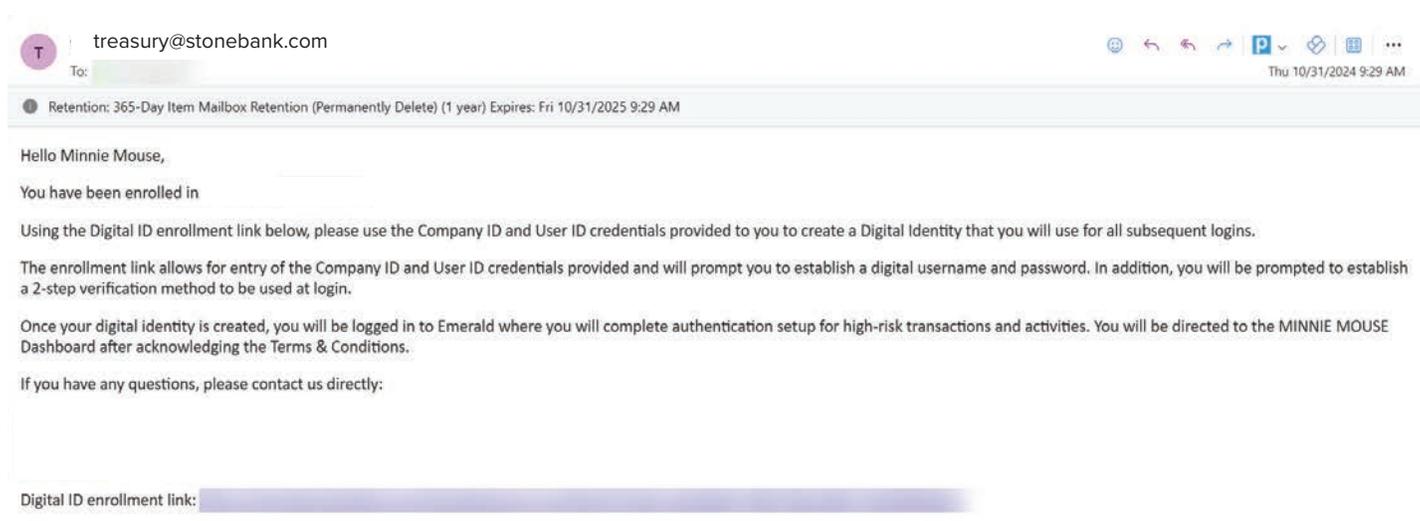
# EMERALD TREASURY MANAGEMENT SERVICES

## DIGITAL UPGRADE FIRST-TIME LOGIN INSTRUCTIONS

### CREATE YOUR STONE BANK ID

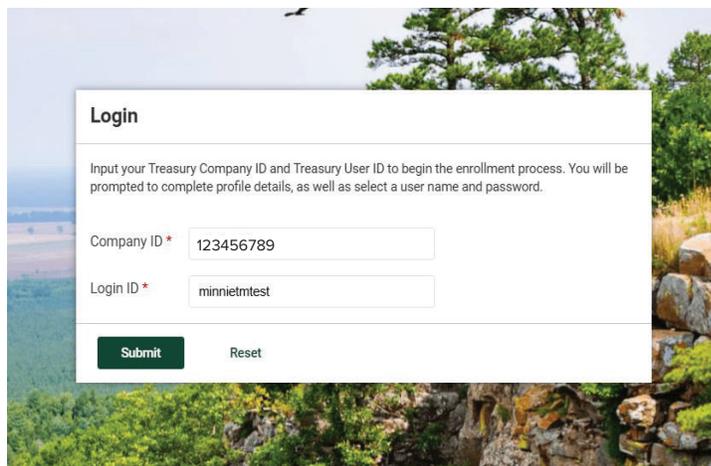
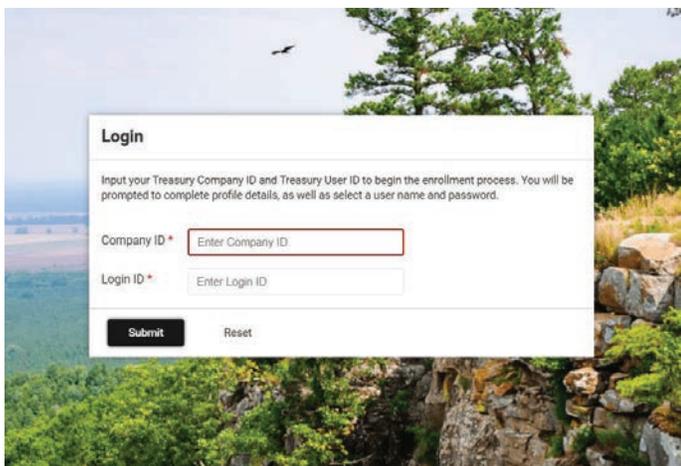
You will receive an enrollment email. This email will include a first-time login link.

You will need your **Company ID (EIN)** and your **Treasury User ID** to login.

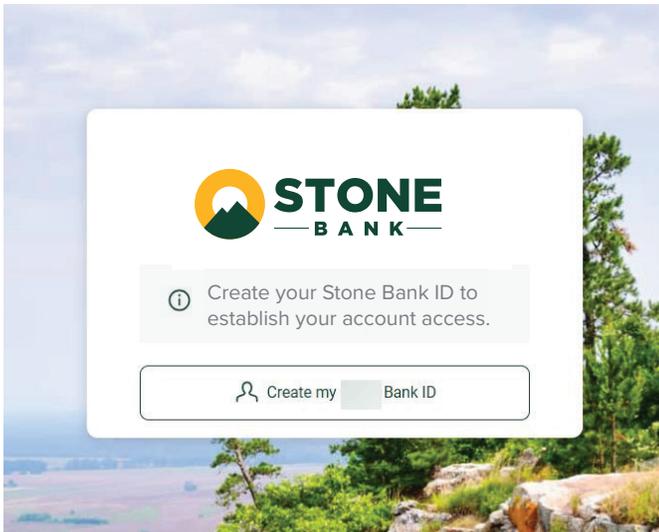


Click the link in the email and input your **Company ID (EIN)** and **Treasury User ID**.

Click **“Submit.”**



Click "Create my Stone Bank ID"



Fill out the form with your information.

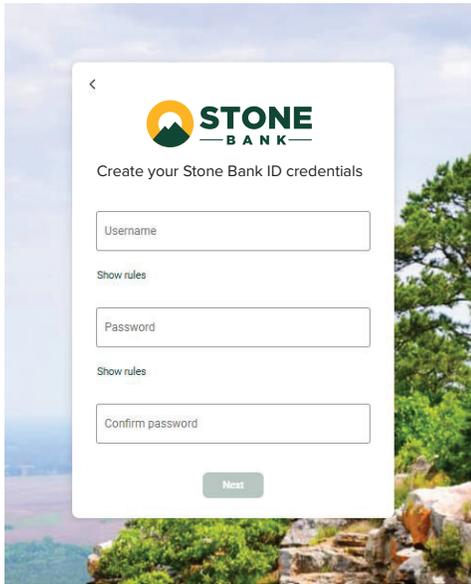
A screenshot of the Stone Bank app showing a form to verify profile information. The form includes fields for First name (Required), Last name (Required), Email (Required), and three Phone Number entries (Home, Mobile, Work). Each phone number entry has a Country dropdown set to "+1" and "US/Canada". A "Next" button is at the bottom.A screenshot of the Stone Bank app showing the same profile information form as the previous one, but with sample data entered. The First name is "Minnie", the Last name is "Mouse", and the Work phone number is "+11111111111". The "Next" button is now highlighted in green.

Member FDIC, Equal Housing Lender

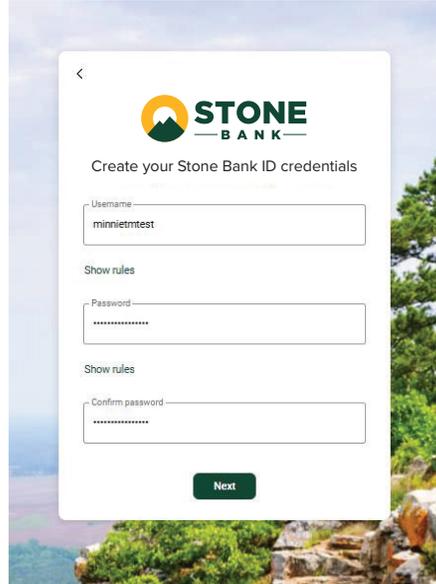
## CREATE YOUR CREDENTIALS

This will include creating a username and inputting a password twice.

Click **“Next”**



The screenshot shows the first step of creating credentials. At the top is the Stone Bank logo and the text "Create your Stone Bank ID credentials". Below this are three input fields: "Username", "Password", and "Confirm password". Each field has a "Show rules" link to its left. A green "Next" button is located at the bottom right of the form.

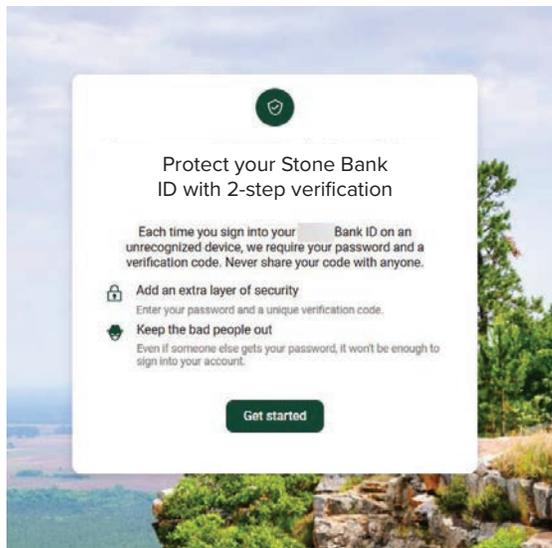


The screenshot shows the second step of creating credentials. The "Username" field is now populated with "minimtest". The "Password" and "Confirm password" fields are filled with masked characters (dots). The "Next" button is now highlighted in green.

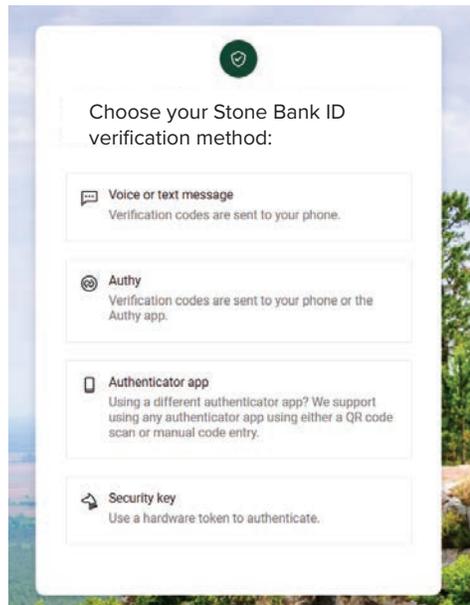
## SET UP YOUR 2-STEP VERIFICATION.

Click **“Get Started”**

You will choose from a list of options to use for your login 2-Step Verification. Select your choice and follow the prompts.



The screenshot shows the first step of setting up 2-step verification. It features the Stone Bank logo and the heading "Protect your Stone Bank ID with 2-step verification". Below the heading is explanatory text: "Each time you sign into your Stone Bank ID on an unrecognized device, we require your password and a verification code. Never share your code with anyone." There are two bullet points: "Add an extra layer of security" (with a lock icon) and "Keep the bad people out" (with a shield icon). A green "Get started" button is at the bottom.

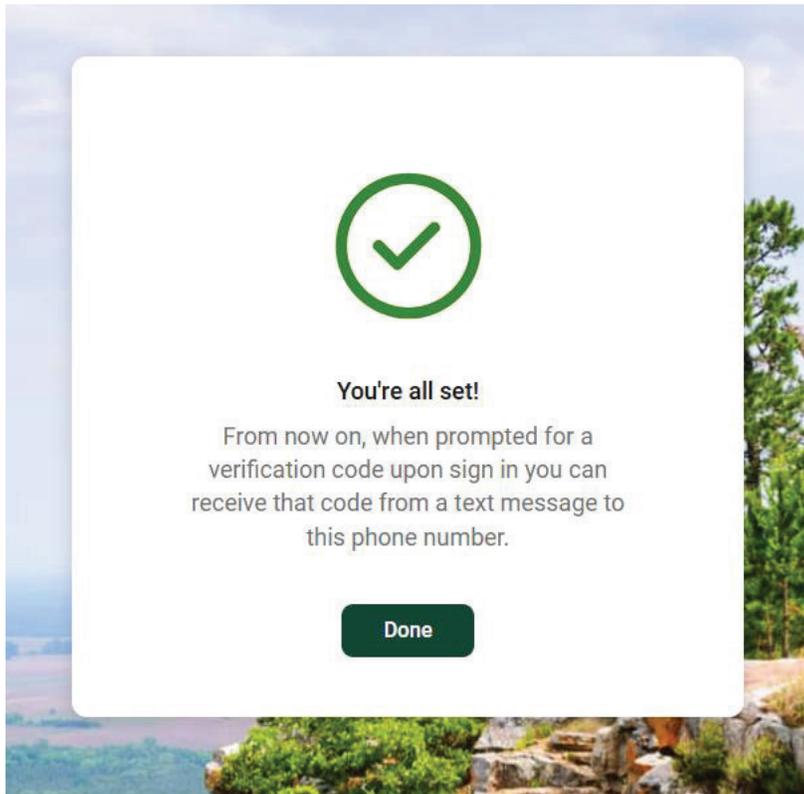


The screenshot shows the second step of setting up 2-step verification. It asks the user to "Choose your Stone Bank ID verification method:". There are four options listed in rounded rectangular boxes: "Voice or text message" (with a speech bubble icon), "Authy" (with a checkmark icon), "Authenticator app" (with a smartphone icon), and "Security key" (with a key icon). Each option includes a brief description of how it works.



Once login 2FA is setup, you will get a confirmation.

Click “**Done**”



## SETUP AUTHENTICATION METHOD

You must now setup your Authentication Method for any high risk actions (ACH, wires, etc).

Depending on the company, this could be Out of Bound (text/phone call) or a Symantec Token.

*Continued on next page.*



Member FDIC, Equal Housing Lender

Out of Bound: Select the **“Add Phone Number”** option for either Text Message or Automated Phone call to receive the secure access code.

Enter in the number and click **“Verify Number”**.

For authentication purposes when working with transactions, please provide phone numbers to receive text messages (SMS) and automated phone calls. You may be prompted to verify your identity by responding to a text message or automated phone call when working with transactions within the Treasury Management platform.

**Text Message (SMS)**

Get a prompt via text message and reply to verify your identity.

**Add Phone Number**

**Automated Phone Call**

Receive a prompt via automated phone call and reply to verify your identity.

**Add Phone Number**

You can only enter this information one time. You must contact your financial institution to change your security phone numbers.

**Done**

**Add Phone Number**

Receive a text message (SMS) and reply to verify your identity.

Phone Number:  -  -

Use same number for automated phone calls

**Verify Number**    **Cancel**

You can only enter this information one time. You must contact your financial institution to change your security phone numbers.

Enter the code received and click **“Verify Number”**

**Verify Phone Number**

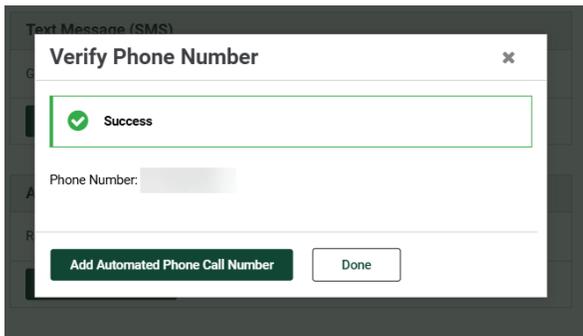
A text message (SMS) was sent to your phone. We need to verify your identity for the security of the account. Please enter your One Time Password below.

Phone number:

**Verify Number**    **Cancel**

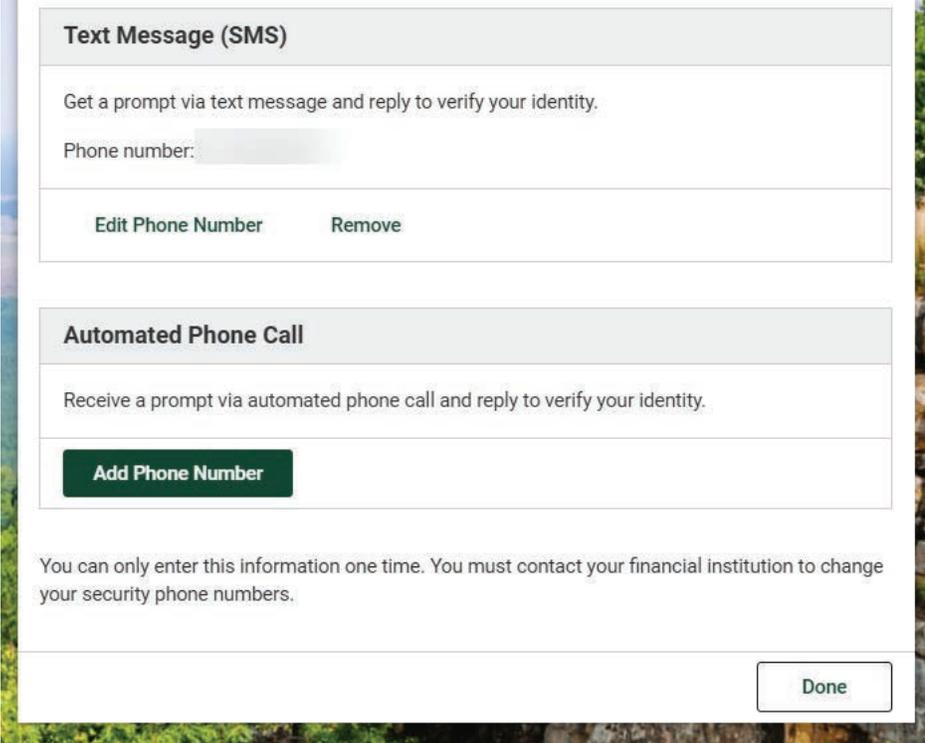


Click **“Done”**



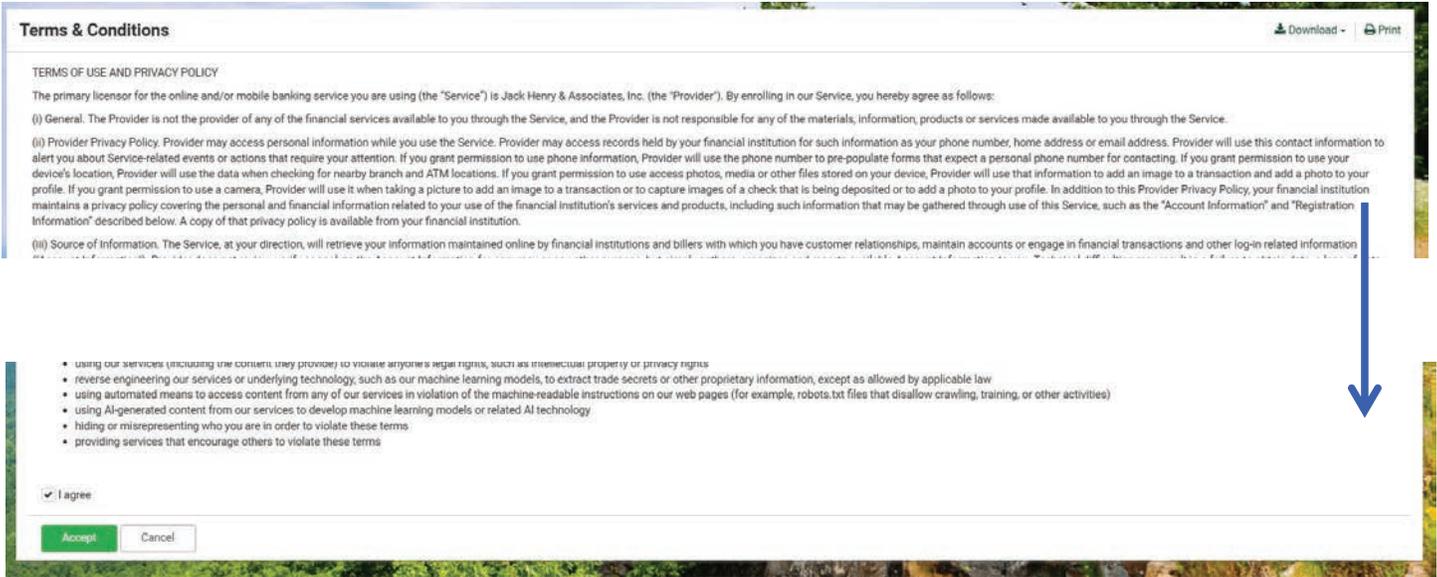
Click **“Done”**

For authentication purposes when working with transactions, please provide phone numbers to receive text messages (SMS) and automated phone calls. You may be prompted to verify your identity by responding to a text message or automated phone call when working with transactions within the Treasury Management platform.



Member FDIC, Equal Housing Lender

Scroll to the bottom to accept the terms and conditions.



**Terms & Conditions** Download Print

**TERMS OF USE AND 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 Information" and "Registration Information" described below. A copy of that privacy policy is available from your financial institution.

(iii) Source of Information. The Service, at your direction, will retrieve your information maintained online by financial institutions and billers with which you have customer relationships, maintain accounts or engage in financial transactions and other log-in related information

- using our services (including the content they provide) to violate anyone's legal rights, such as intellectual property or privacy rights
- reverse engineering our services or underlying technology, such as our machine learning models, to extract trade secrets or other proprietary information, except as allowed by applicable law
- using automated means to access content from any of our services in violation of the machine-readable instructions on our web pages (for example, robots.txt files that disallow crawling, training, or other activities)
- using AI-generated content from our services to develop machine learning models or related AI technology
- hiding or misrepresenting who you are in order to violate these terms
- providing services that encourage others to violate these terms

I agree

## IF YOU HAVE QUESTIONS OR NEED ASSISTANCE

Please don't hesitate to contact us at (833) 253-2265 or via email at [CustomerService@StoneBank.com](mailto:CustomerService@StoneBank.com).

This and other guides can be found online at [stonebank.com/digital-upgrade](https://stonebank.com/digital-upgrade)



Member FDIC, Equal Housing Lender