First-Time Secure Login for Treasury Management Users

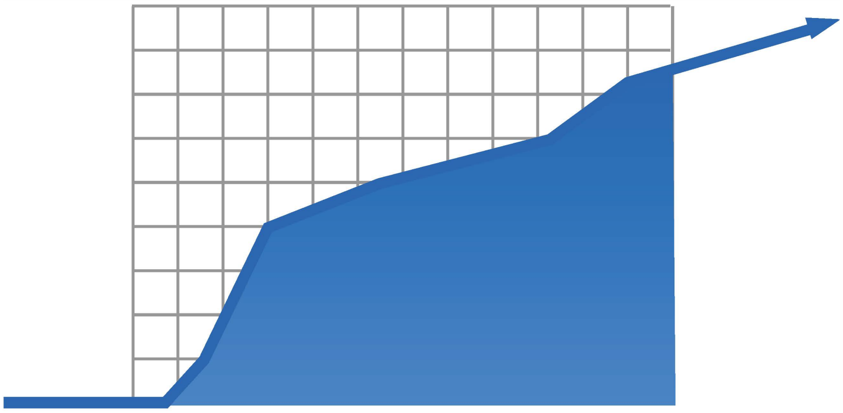
Let us be your guide.

For good reason, First-Time login to our Commercial Online Banking platform is a secure process.

Each user is empowered with the ability to customize their own unique User Login credentials. Administrators can determine when passwords expire and set deadlines for users to reset their passwords. In addition to these user friendly features, we have created a process to ensure first-time logins will be secure across your organization. This Guide will walk you through each step. From Enrollment to first-time credential settings, to establishing security questions, you'll be prepared to educate your team members as well as provide orientation for new associates.

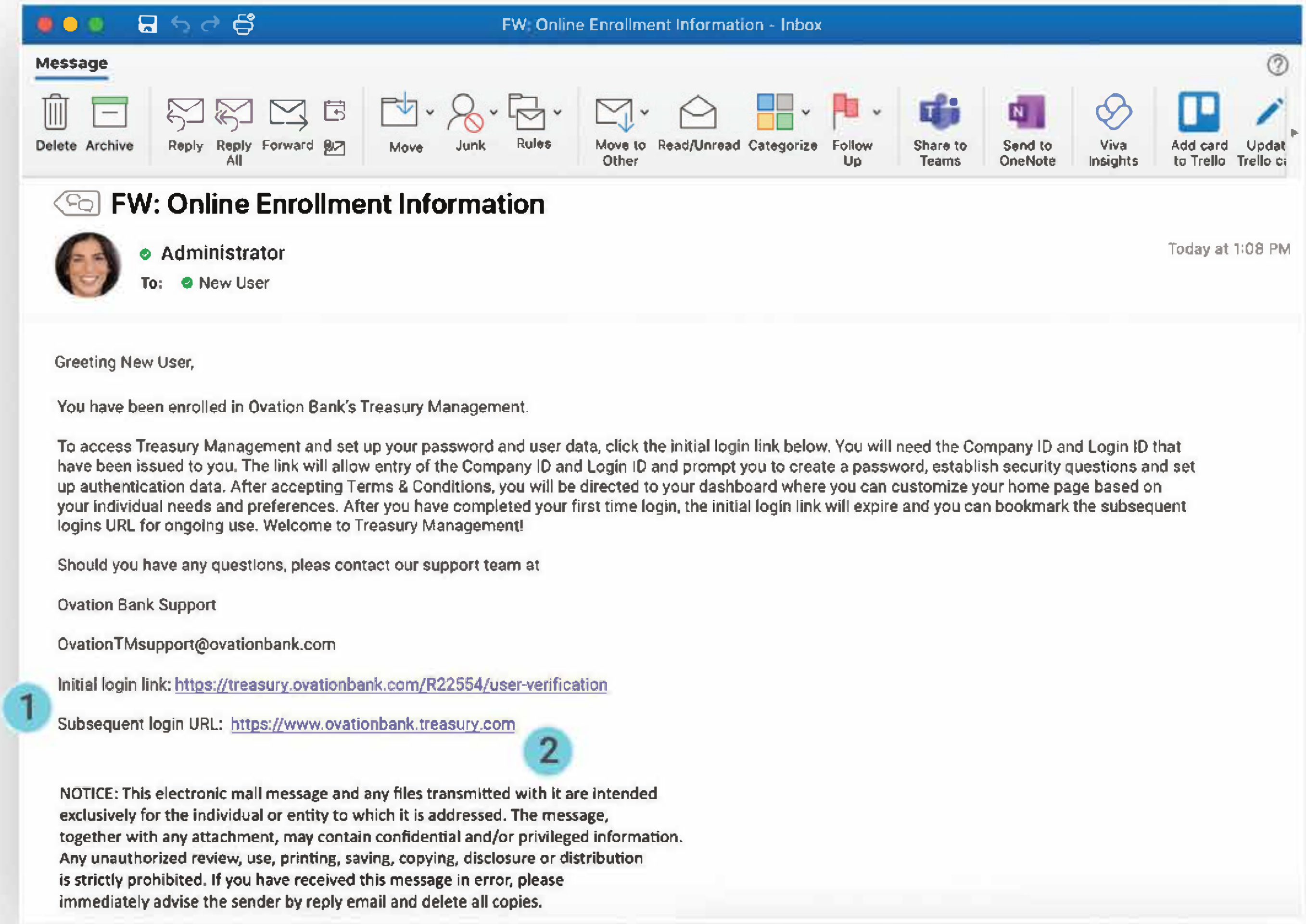
Let us guide you through each of these **7 easy to follow steps:**

Step 1 Enrollment email
Step 2 Credentials for first time login
Step 3 Completing a first login
Step 4 Enroll SMS text or Token authentication
Step 5 Creating a new password
Step 6 Establishing security questions
Step 7 Accepting Terms and Conditions



Step 1: Enrollment Email

When a new user is created by a company administrator, an email will be sent as soon as the enrollment is completed. The email will contain a link to be used for the first-time login. This link can only be used for the first login. After the user has successfully signed in, the link will no longer be valid. From the time the email has been delivered, the user will have no more than seven days to complete the initial login. After seven days, the link will expire.



FW: Online Enrollment Information

Administrator

To: New User

Today at 1:08 PM

Greeting New User,

You have been enrolled in Ovation Bank's Treasury Management.

To access Treasury Management and set up your password and user data, click the initial login link below. You will need the Company ID and Login ID that have been issued to you. The link will allow entry of the Company ID and Login ID and prompt you to create a password, establish security questions and set up authentication data. After accepting Terms & Conditions, you will be directed to your dashboard where you can customize your home page based on your individual needs and preferences. After you have completed your first time login, the initial login link will expire and you can bookmark the subsequent logins URL for ongoing use. Welcome to Treasury Management!

Should you have any questions, pleas contact our support team at

Ovation Bank Support

OvationTMsupport@ovationbank.com

Initial login link: https://treasury.ovationbank.com/R22554/user-verification

Subsequent login URL: https://www.ovationbank.treasury.com

NOTICE: This electronic mail message and any files transmitted with it are intended exclusively for the individual or entity to which it is addressed. The message, together with any attachment, may contain confidential and/or privileged information. Any unauthorized review, use, printing, saving, copying, disclosure or distribution is strictly prohibited. If you have received this message in error, please immediately advise the sender by reply email and delete all copies.

1 **Initial Login Link** will take the user through several enrollment and authentications steps.

2 **Login Link** will will be used for logins after the enrollment process. We recommend bookmarking it so it is alway assessable.

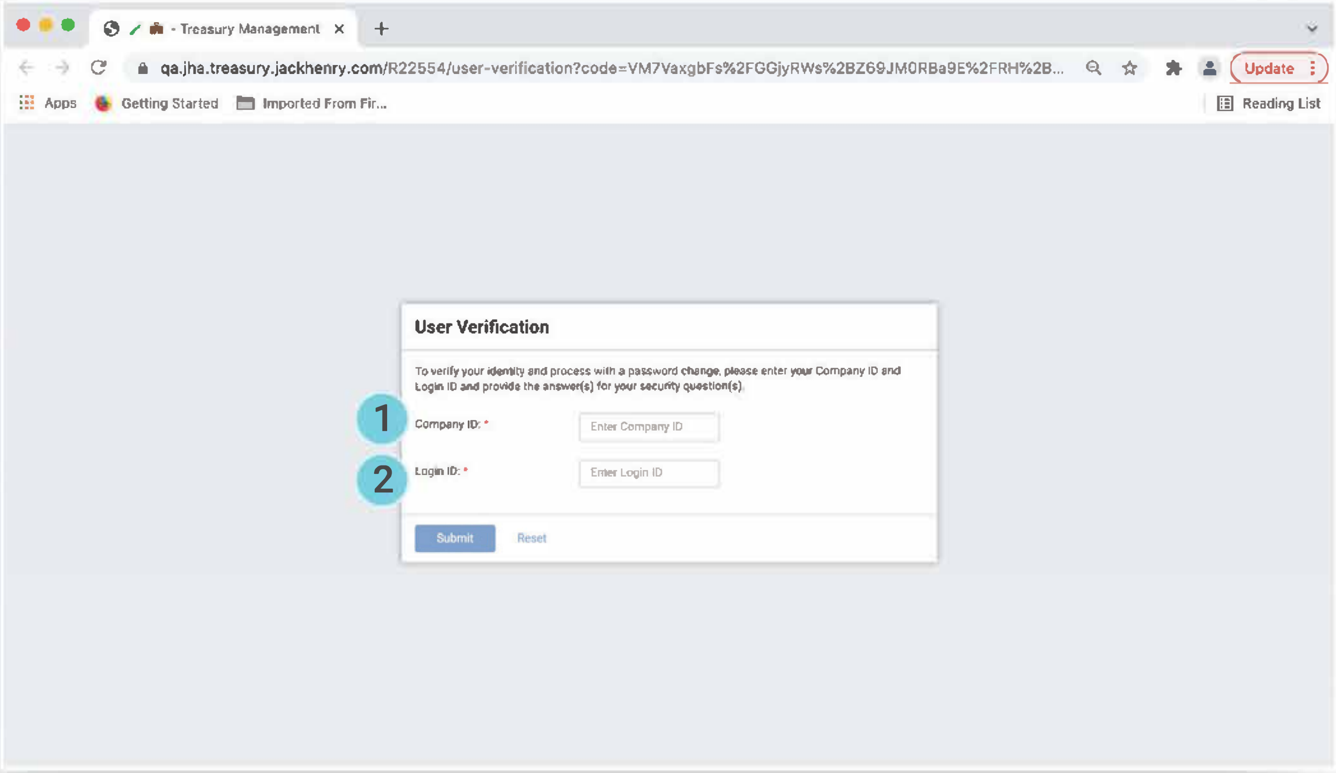
Note: Enroll email for converted users.

During our conversion event, each user will receive two emails on Monday, November 11th after 8am, a welcome email containing your Company ID and an enrollment email. Each user should click on the Initial login link in the enrollment email, use the Company ID provided and follow the instructions for login.

Step 2: Credentials for first time login

The initial login link in the enrollment email is the user's gateway to the platform. However, there is required information for a successful login that must be communicated to the user before the email is sent. We will create the company ID when onboarding your company in our Back Office. This company ID is part of every login, including the initial login, and must be known to the user at that time.

We may leverage many different options for communicating the company and login ID credentials. During our conversion event, individualized mailings to users to communicate the company ID and enrollment links will be sent. For ongoing business, methods such as secure email or personalized training (on-site or remote) are common practices for communicating the required credentials.


- Treasury Management
qa.jha.treasury.jackhenry.com/R22554/user-verification?code=VM7VaxgbFs%2FGGjyRWs%2BZ69JM0RBa9E%2FRH%2B...
Update
Apps
Getting Started
Imported From Fir...
Reading List

User Verification

To verify your identity and process with a password change, please enter your Company ID and Login ID and provide the answer(s) for your security question(s).

1 Company ID: * Enter Company ID

2 Login ID: * Enter Login ID

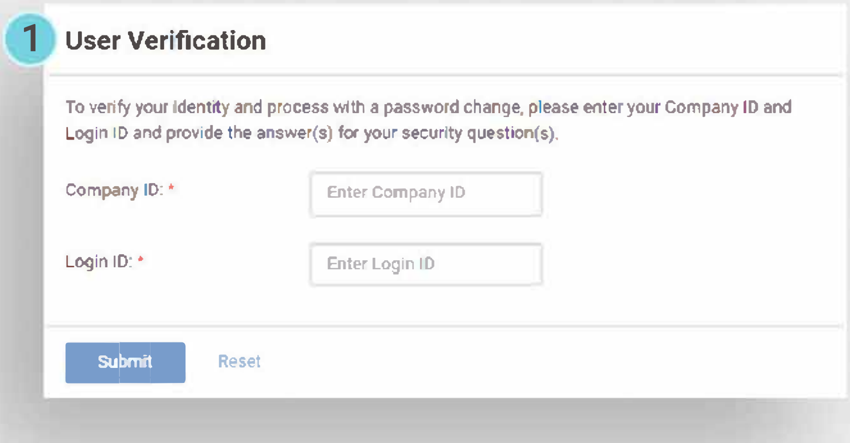
1 Company ID is generated by the Bank in our Back Office. The bank will need to provide this information to the selected admins at each company. Due to its secure nature, verbal disclosure or encrypted communication is recommended.

2 Login ID is specific to each individual user. This too must be communicated **before** the enrollment email is sent in order for a success login to be completed. Again due to its secure nature, verbal disclosure or encrypted communication is recommended.

Step 3: Completing a first login

Once a user is in possession of his or her credentials and the enrollment email has been sent, login can occur. There are several steps required during this process. The first time the user logs in, he or she will be guided through the procedures listed below.

Accessing Initial login



User Verification

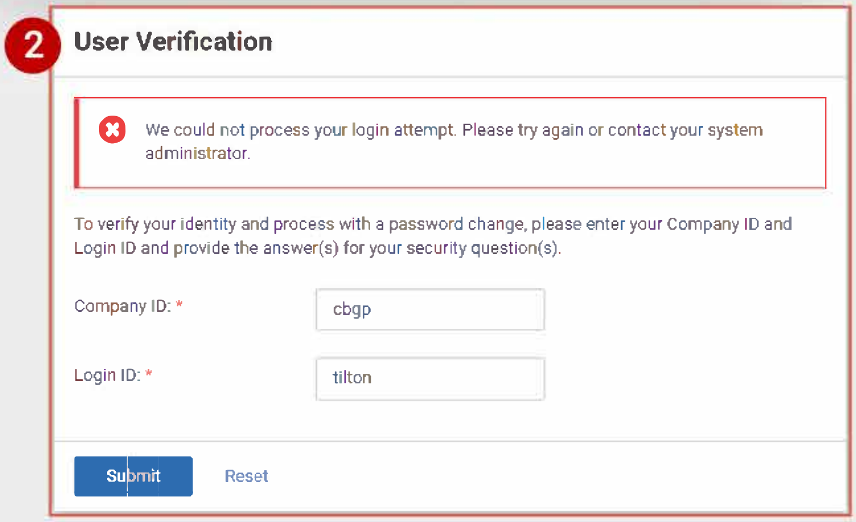
To verify your identity and process with a password change, please enter your Company ID and Login ID and provide the answer(s) for your security question(s).

Company ID: * Enter Company ID

Login ID: * Enter Login ID

1. First Prompt

The initial login screen is accessed via the link on the enrollment email. On landing, the user will be prompted to enter the company ID and Login ID.



User Verification

We could not process your login attempt. Please try again or contact your system administrator.

To verify your identity and process with a password change, please enter your Company ID and Login ID and provide the answer(s) for your security question(s).

Company ID: * cbgp

Login ID: * tilton

2 Error Scenario

If the credentials entered are not valid, the user will receive an error. The user can re-attempt by correcting the invalid data and re-submitting.

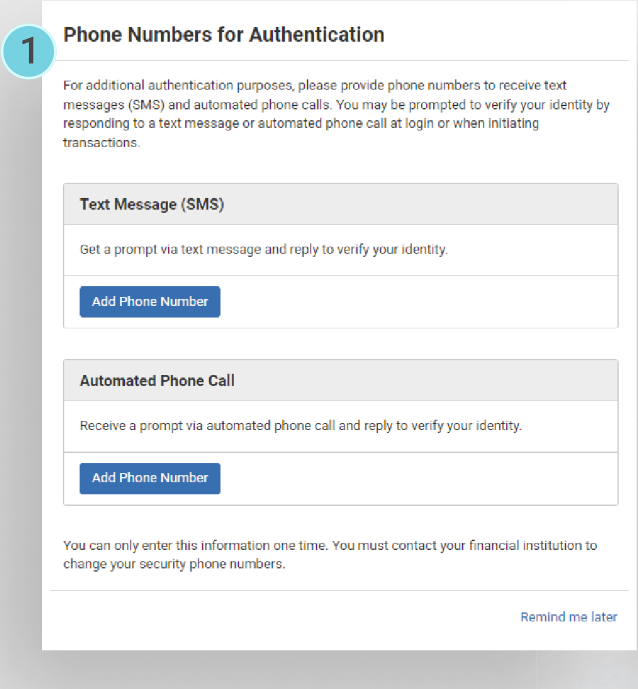
The remainder of this guide will focus on these final steps.

- ✓ Enrolling for SMS text or token authentication
- ✓ Creating a new password
- ✓ Establishing security questions and answers
- ✓ Accepting Terms and Conditions

Step 4: Enrolling SMS Authentication

After the company ID and login ID are validated, the user will be guided through the collection process for Out of Band or Token authentication.

1



Phone Numbers for Authentication

For additional authentication purposes, 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 at login or when initiating transactions.

Text Message (SMS)

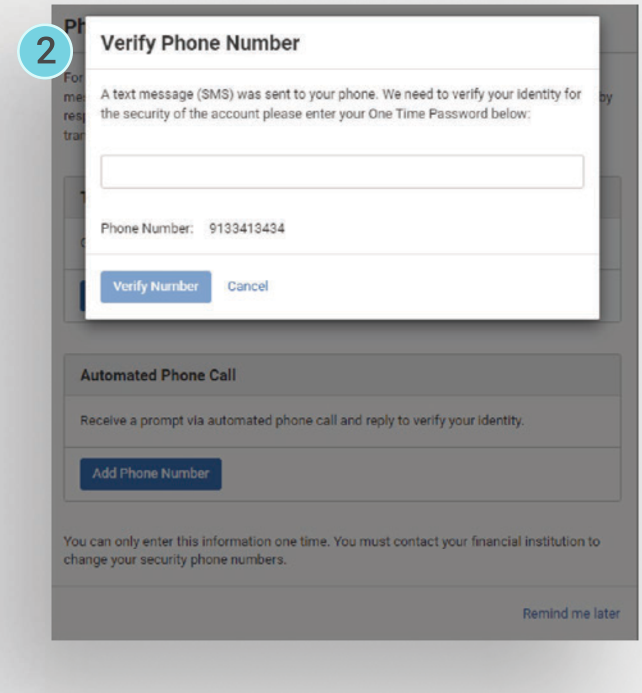
Get a prompt via text message and reply to verify your identity.

Automated Phone Call

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

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

2



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: 9133413434

Automated Phone Call

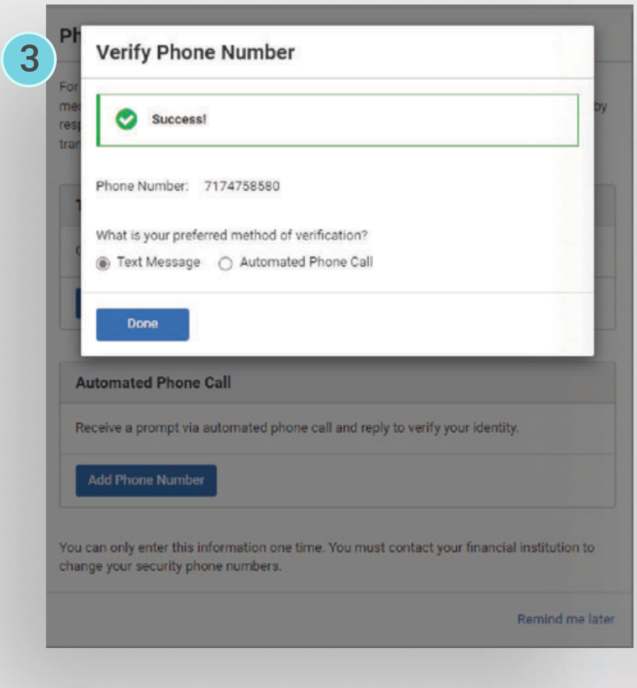
Receive a prompt via automated phone call and reply to verify your identity.

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

1. First Prompt For out of band (SMS text or phone call) the user will be prompted to add a number. When a number is added, a code will be sent to the mobile device in case of text or delivered via automated phone call.

2. Second Prompt The code must then be entered into the verification screen and it must be an exact match for the code that was delivered to the user’s phone. The code will be valid for no more than 10 minutes.

Step 4: Enrolling SMS Authentication



3

Verify Phone Number

Success!

Phone Number: 7174758580

What is your preferred method of verification?

● Text Message ○ Automated Phone Call

Done

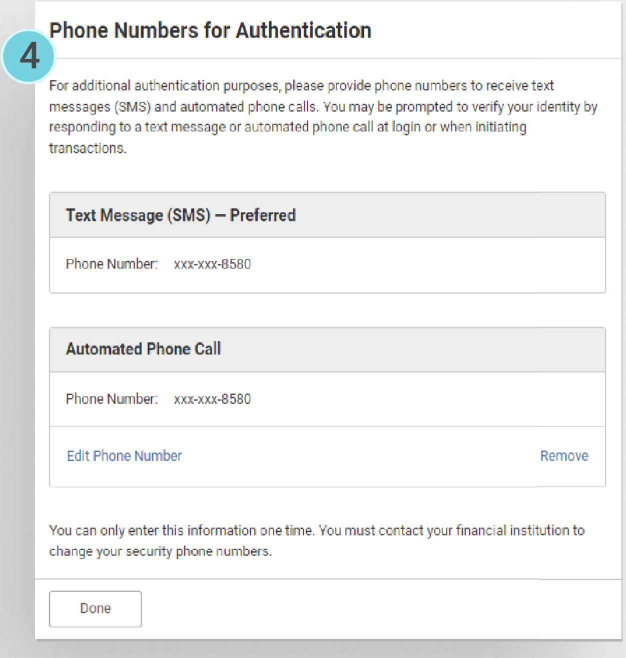
Automated Phone Call

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.

Remind me later



4

Phone Numbers for Authentication

For additional authentication purposes, 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 at login or when initiating transactions.

Text Message (SMS) – Preferred

Phone Number: xxx-xxx-8580

Automated Phone Call

Phone Number: xxx-xxx-8580

Edit Phone Number

Remove

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

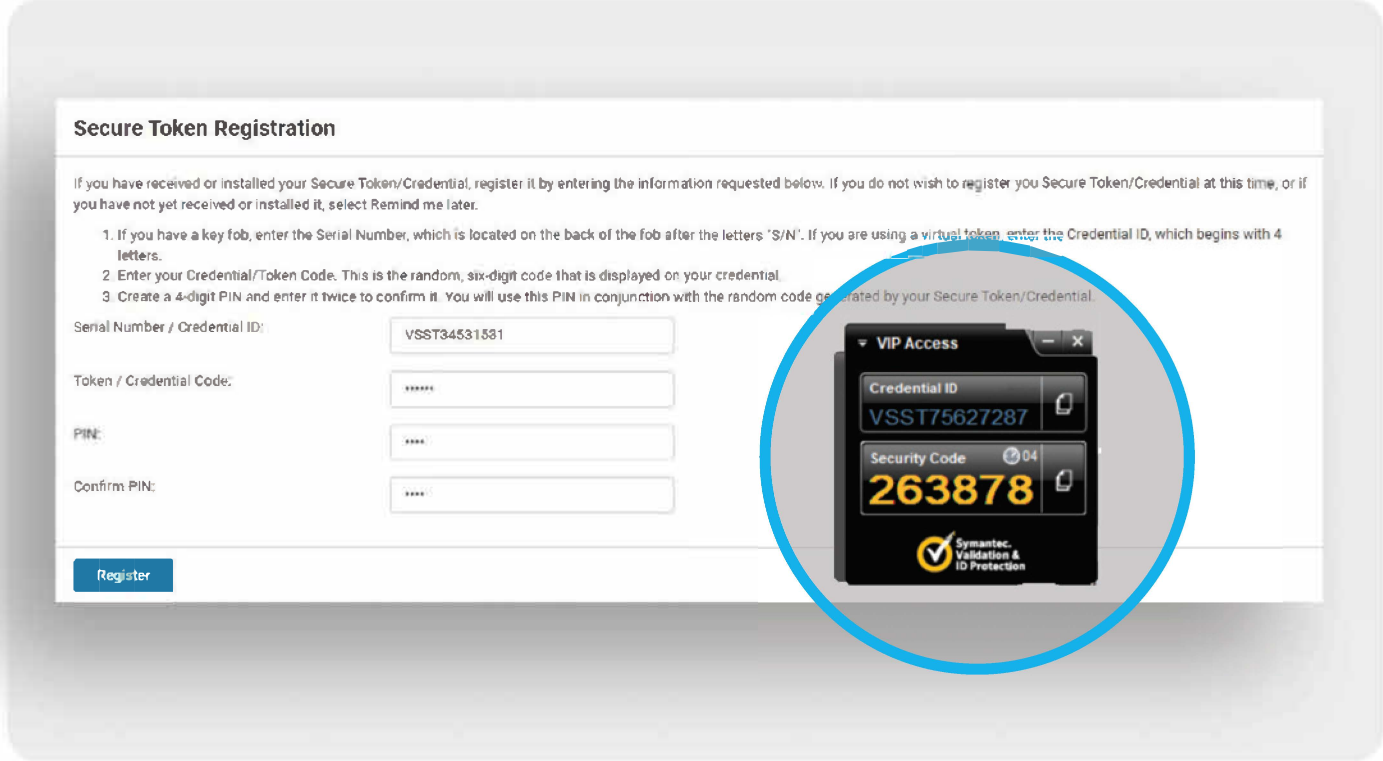
Done

3. Third Prompt When the code is entered and validated, the user will then have option to use the same number for either text or automated phone call, and set the preferred method.

4. Fourth Prompt The final step allows the user to complete the authentication collection and continue, or continue to add / edit authentication data. After clicking Done, the user will continue to the next phase of the first time login.

Step 4: Token Authentication for ACH and Wires

For clients set up for token authentication, step four will collect the token data in lieu of a phone number for text authentication. Token authentication is completed in one simple step. The token, which can be a mobile application, PC desktop application, or physical device, will have a serial number. This serial number or device ID must be entered in the token registration screen, along with the one-time code currently displayed on the token. Each user will also personalize a four-digit PIN that will be included after the token code each time authentication is required.



Secure Token Registration

If you have received or installed your Secure Token/Credential, register it by entering the information requested below. If you do not wish to register you Secure Token/Credential at this time, or if you have not yet received or installed it, select Remind me later.

1. If you have a key fob, enter the Serial Number, which is located on the back of the fob after the letters 'S/N'. If you are using a virtual token, enter the Credential ID, which begins with 4 letters.
2. Enter your Credential/Token Code. This is the random, six-digit code that is displayed on your credential.
3. Create a 4-digit PIN and enter it twice to confirm it. You will use this PIN in conjunction with the random code generated by your Secure Token/Credential.

Serial Number / Credential ID:	VSST34531531
Token / Credential Code:	••••••
PIN:	••••
Confirm PIN:	••••

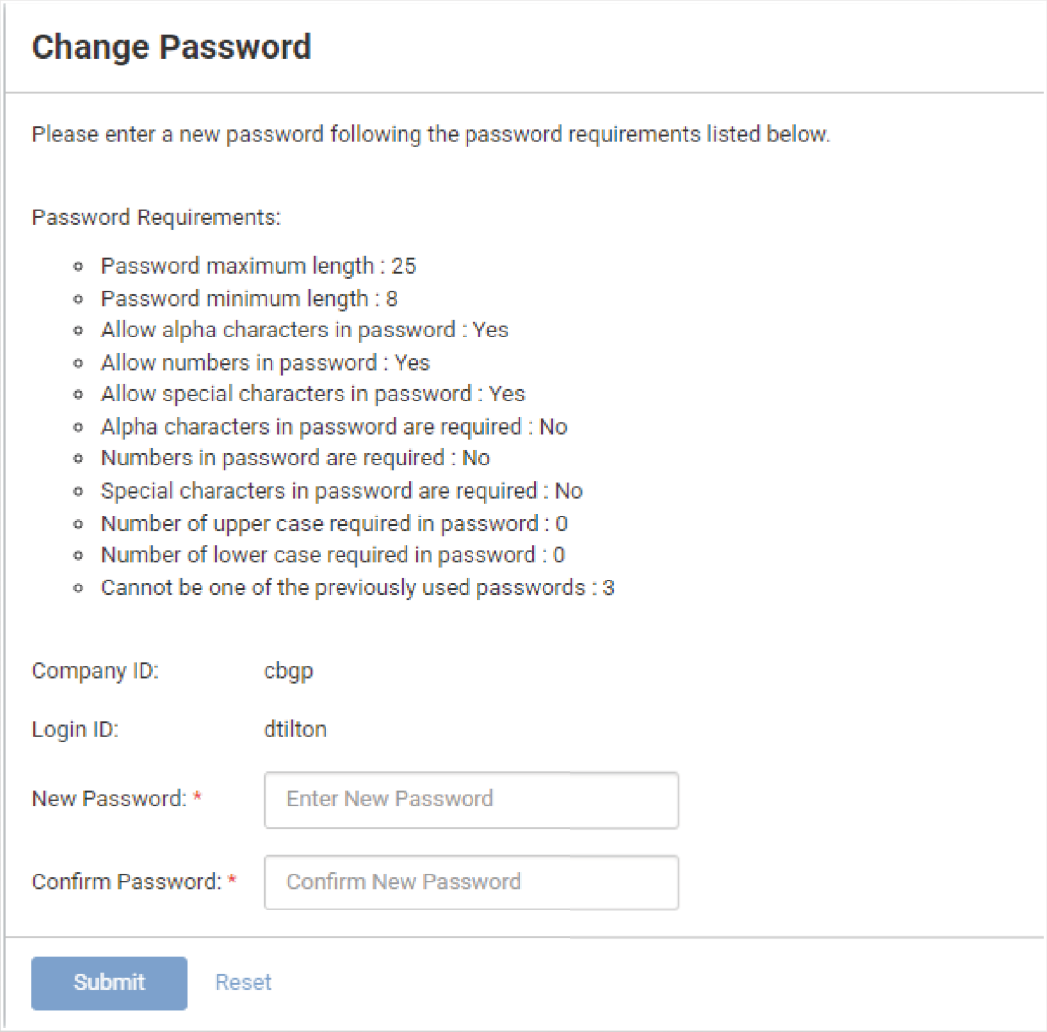
Credential ID
VSST75627287

Security Code 04
263878

Note: If you have not yet downloaded a token, you can download an application to your PC by visiting https://vip.symantec.com. If you prefer to use a mobile device application, search for VIP Access (Symantec VIP) in your device application store.

Step 5: Creating a new password

During the initial login process, the user does not have or use a temporary password. For continued use, a password must be created. The password parameters are established by the financial institution in Back Office and each institution may set requirements differently.



Change Password

Please enter a new password following the password requirements listed below.

Password Requirements:

- Password maximum length : 25
- Password minimum length : 8
- Allow alpha characters in password : Yes
- Allow numbers in password : Yes
- Allow special characters in password : Yes
- Alpha characters in password are required : No
- Numbers in password are required : No
- Special characters in password are required : No
- Number of upper case required in password : 0
- Number of lower case required in password : 0
- Cannot be one of the previously used passwords : 3

Company ID: cbgp

Login ID: dtilton

New Password: * Enter New Password

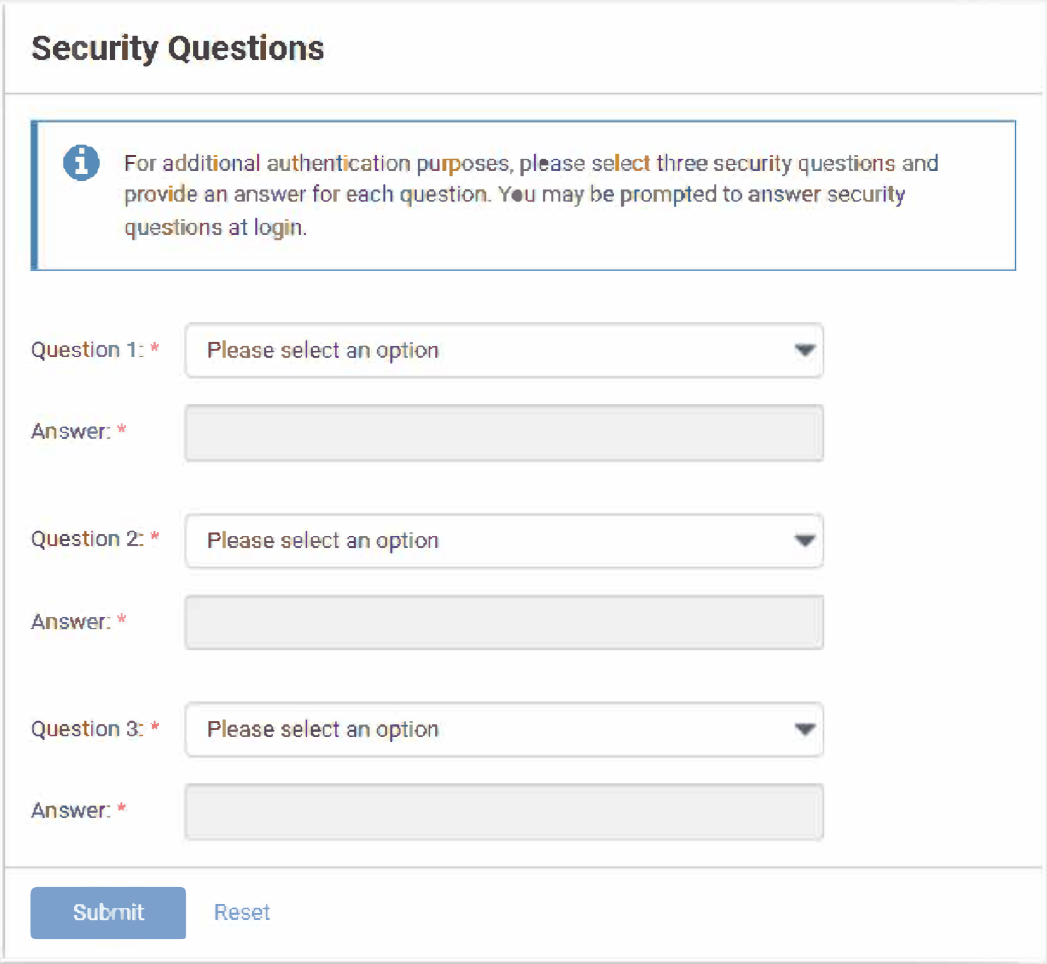
Confirm Password: * Confirm New Password

Password Strength For password strength, the password should be no less than eight characters and should require combinations of alpha, numeric and special characters. Passwords are case sensitive so it is also advisable to require a specific number of uppercase alpha characters.

Note: The requirements will be displayed to the user on the screen and the user will not be able to save until the entered data satisfies the requirements. To ensure that the user has entered a string that he or she intended to, **it must be entered twice.**

Step 6: Security questions and answers

The Commercial Online Banking platform uses RSA to challenge users with security questions if anomalies are detected in a login session. Completing security question registration is part of the initial login process. Each user must select three questions and fill in the corresponding answer.



Security Questions

For additional authentication purposes, please select three security questions and provide an answer for each question. You may be prompted to answer security questions at login.

Question 1: * Please select an option

Answer: *

Question 2: * Please select an option

Answer: *

Question 3: * Please select an option

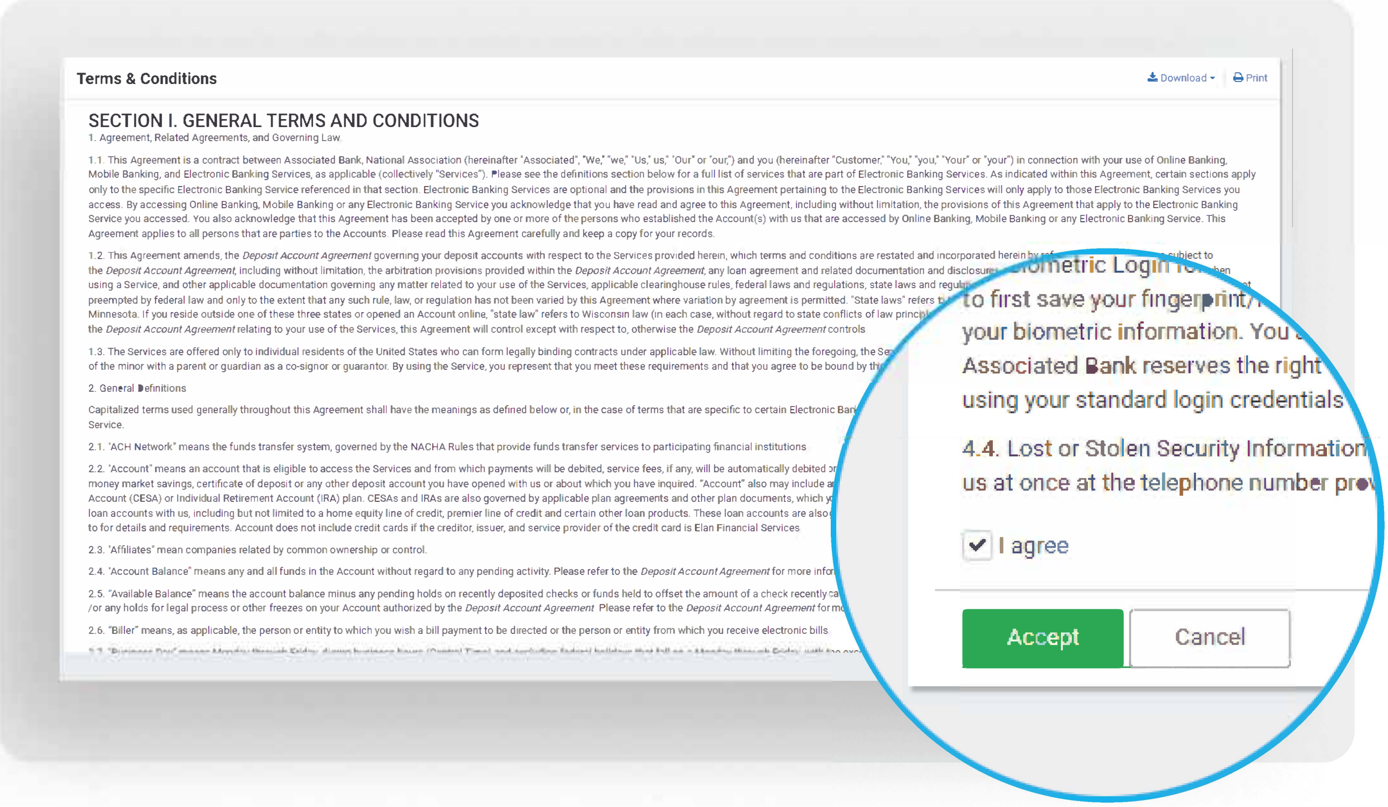
Answer: *

Hint: The questions selected should be appropriate to the user and the answers should be information the user can easily recall for authentication at random times.

Note: A user cannot opt-out or bypass security question registration. This is a requirement to use the platform.

Step 7: Accepting Terms and Conditions

Terms & Conditions for the Commercial Online Banking system are controlled by a Bank back office user. The terms can be updated at any time and the Bank can choose to have all users re-accept any time a change is made. All users signing into Commercial Online Banking must accept the Bank's Terms & Conditions. There are no options to defer or decline. If a user does not complete the acceptance, the session will be terminated. To accept Terms & Conditions, the user must scroll to the bottom of the document



Terms & Conditions

SECTION I. GENERAL TERMS AND CONDITIONS

1. Agreement, Related Agreements, and Governing Law

1.1. This Agreement is a contract between Associated Bank, National Association (hereinafter "Associated", "We," "we," "Us," us," "Our" or "our,") and you (hereinafter "Customer," "You," "you," "Your" or "your") in connection with your use of Online Banking, Mobile Banking, and Electronic Banking Services, as applicable (collectively "Services"). Please see the definitions section below for a full list of services that are part of Electronic Banking Services. As indicated within this Agreement, certain sections apply only to the specific Electronic Banking Service referenced in that section. Electronic Banking Services are optional and the provisions in this Agreement pertaining to the Electronic Banking Services will only apply to those Electronic Banking Services you access. By accessing Online Banking, Mobile Banking or any Electronic Banking Service you acknowledge that you have read and agree to this Agreement, including without limitation, the provisions of this Agreement that apply to the Electronic Banking Service you accessed. You also acknowledge that this Agreement has been accepted by one or more of the persons who established the Account(s) with us that are accessed by Online Banking, Mobile Banking or any Electronic Banking Service. This Agreement applies to all persons that are parties to the Accounts. Please read this Agreement carefully and keep a copy for your records.

1.2. This Agreement amends, the *Deposit Account Agreement* governing your deposit accounts with respect to the Services provided herein, which terms and conditions are restated and incorporated herein by ref
subject to
the *Deposit Account Agreement*, including without limitation, the arbitration provisions provided within the *Deposit Account Agreement*, any loan agreement and related documentation and disclosur
hen
using a Service, and other applicable documentation governing any matter related to your use of the Services, applicable clearinghouse rules, federal laws and regulations, state laws and regul
preempted by federal law and only to the extent that any such rule, law, or regulation has not been varied by this Agreement where variation by agreement is permitted. "State laws" refers t
Minnesota. If you reside outside one of these three states or opened an Account online, "state law" refers to Wisconsin law (in each case, without regard to state conflicts of law princi
the *Deposit Account Agreement* relating to your use of the Services, this Agreement will control except with respect to, otherwise the *Deposit Account Agreement* controls

1.3. The Services are offered only to individual residents of the United States who can form legally binding contracts under applicable law. Without limiting the foregoing, the Se
of the minor with a parent or guardian as a co-signor or guarantor. By using the Service, you represent that you meet these requirements and that you agree to be bound by th

2. General Definitions

Capitalized terms used generally throughout this Agreement shall have the meanings as defined below or, in the case of terms that are specific to certain Electronic Ban
Service.

2.1. "ACH Network" means the funds transfer system, governed by the NACHA Rules that provide funds transfer services to participating financial institutions

2.2. "Account" means an account that is eligible to access the Services and from which payments will be debited, service fees, if any, will be automatically debited or
money market savings, certificate of deposit or any other deposit account you have opened with us or about which you have inquired. "Account" also may include a
Account (CESA) or Individual Retirement Account (IRA) plan. CESAs and IRAs are also governed by applicable plan agreements and other plan documents, which y
loan accounts with us, including but not limited to a home equity line of credit, premier line of credit and certain other loan products. These loan accounts are also
to for details and requirements. Account does not include credit cards if the creditor, issuer, and service provider of the credit card is Elan Financial Services

2.3. "Affiliates" mean companies related by common ownership or control.

2.4. "Account Balance" means any and all funds in the Account without regard to any pending activity. Please refer to the *Deposit Account Agreement* for more infor

2.5. "Available Balance" means the account balance minus any pending holds on recently deposited checks or funds held to offset the amount of a check recently ca
/or any holds for legal process or other freezes on your Account authorized by the *Deposit Account Agreement* Please refer to the *Deposit Account Agreement* for mo

2.6. "Biller" means, as applicable, the person or entity to which you wish a bill payment to be directed or the person or entity from which you receive electronic bills

ometric Login fo
to first save your fingerprint/
your biometric information. You
Associated Bank reserves the right
using your standard login credentials

4.4. Lost or Stolen Security Information
us at once at the telephone number prov

☑ I agree

Accept and Agree After scrolling to the bottom of the Terms & Conditions, there are two required actions to complete the acceptance. First, the user must check the I agree box. Second, the user must click Accept. This completes the first time login process.

During the subsequent logins, the user will access the institution's conventional login page and authenticate with

- **Company ID**
- **Login ID**
- **Password**

If the Bank requires additional authentication at login (with token or SMS text) the challenge will occur after the company ID / Login ID / Password have been validated. Additionally, if anomalies are detected such as logging in from a different location or a dynamic IP address, the user may be challenged with security questions.

Let’s keep the conversation going. For more information on ACH, wires, reporting or our cash management platform in general, contact us.

Burke&Herbert Bank

treasuryservices@burkeandherbertbank.com