Marine Bank

WE'RE TAKING SECURITY TO THE NEXT LEVEL FOR CASH MANAGEMENT USERS!

With the ever-changing landscape of technology, and the ever-prevalent presence of fraud, securing your account information has never been more important. Unified Identity Service (UIS) replaces the basic multi-factor authentication service used today and adopts industry-standard authentication methods designed to protect against varying types of online account takeover threats.

Benefits of UIS:

- Identify and block credential stuffing attacks
- Makes it difficult for phishing and other attack schemes to be possible
- Manage multiple profiles with a single identity (if applicable)
- Provides an ongoing benefit of the software's security protocol

What do you need to do?

On May 12th at 9:00am EST, you will receive an email prompting you to create your new Digital Identity.

Note: The email link will only work for 7 days. You will have 45 minutes to complete the process, once you click on the link.

You'll be prompted to create a new digital identity for ongoing access which is a simple four-step process:

1. Click the link provided in the email sent from notifications@marinebank.bank when received on the morning of **May 12th, 2025**.
2. Authenticate with your existing company and login ID.
3. Create a new digital profile, including a unique Username.
4. Establish a new two-factor authentication (2FA) method for account access.

Have questions? Please see the other side for frequently asked questions about Unified Identity Service (UIS).

FAQS

1. **Why is Marine Bank making this change?**
   This upgrade will replace the basic multi-factor authentication service with a more robust platform.
2. **Can I use my current user ID?**
   Usernames now need to be unique across all our online banking platforms. In some cases, a new User ID will have to be chosen. Using a combination of your existing username and Cash Management Company ID will help keep the user ID unique and familiar at the same time.
3. **What are the requirements for creating a new username?**
   Usernames must be between 4 and 64 characters in length. Usernames can contain letters (a-z), numbers (0-9), dashes (-), underscores (_), apostrophes (‘), and periods (.) and can begin or end with non-alphanumeric characters except periods (.) and spaces. Usernames cannot contain more than one period (.) in a row, accents, accented letters, ampersands (&), equal signs (=), brackets (), plus signs (+), at signs (@), or commas (,).
4. **What are the requirements for creating a new password?**
   Passwords must be between 8 and 64 characters in length. Passwords must not match or contain your username and must not begin or end with a space.
5. **What do I do if I have multiple Cash Management logins?**
   If the same email address is tied to multiple Companies, you will receive an individual email for each Company. The first email link clicked will prompt you through the steps to create your digital ID. When you click the link in the second (or third) email, you will be able to use the “Already have a Treasury Bank ID?” Login to link an additional account. Upon entering your Digital ID, you created the first time your accounts will be linked together under that one digital ID. Upon subsequent login, the user will get to choose which company they want to access when logging in.
6. **Will I still need to use my token when initiating an ACH or Wire Payment?**
   There are no changes to this process, and you will authenticate the same as you have before.
7. **How do I log in in the future?**
   If you have the website bookmarked, you will need to update your bookmark to the Cash Management dashboard after you have logged in. Do NOT bookmark the UIS login screen.
8. **If I link to an Intuit product, what action is needed to continue to sync?**
   On Intuit’s side, you will be prompted to log back in with Marine Bank. You will use your new Digital ID and password you created.
9. **Will my new password expire?**
   No, your new password will not expire.
10. **What is a “credential stuffing attack”?**
    Credential stuffing is a cyberattack method in which attackers use lists of compromised user credentials to breach a system. The attack uses bots to automate the effort, and is based on the assumption that many users reuse usernames and passwords across multiple services.

Have Questions?

Contact Cash Management at **772-231-8256**, by email **cashmanagement@marinebank.bank** or send a secure message through your Cash Management online banking.

Marine Bank

MarineBank.bank

EQUAL HOUSING LENDER

Member FDIC