Parkside Financial

BANK & TRUST

Important Update: Treasury Management Platform Transition to Unified Identity Service

On **February 5th, 2024**, the Treasury Management platform will transition to the **Unified Identity Service (UIS)**, which will replace the current Security Question feature.
This change is part of our effort to enhance your security and user experience. While the existing two-factor authentication provides basic security, UIS takes it a step further by offering a more consistent, secure, and robust login process. With UIS, you'll have an upgraded and more reliable way to access your Treasury Management account.

Important Steps for Setting Up Your New Digital Identity
If you're an active user and logged in at least 45 days before the migration date, you'll receive an email with instructions and a link to set up your new Digital Identity. Here's what you need to do:

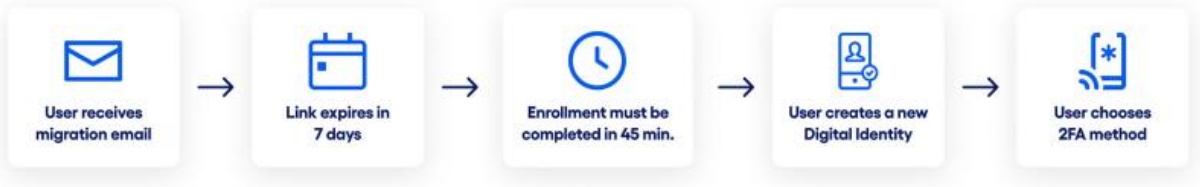
1. **Check Your Email**: You'll get an email with a link to create your new Digital Identity. Be sure to act quickly – the link will expire in 7 days.

2. **Complete Enrollment Within 45 Minutes**: Once you click the link in the email, you'll have 45 minutes to finish setting up your new Digital Identity. If you don't complete it in time, you'll need help from the bank to proceed.

3. **Choose Your New Username and Password**: When you click the link, you'll be asked to create a new username and password. This will be your login for all future sessions.

4. **Set Up Two-Factor Authentication**: After setting your username and password, you'll be asked to choose a two-factor authentication method. This extra layer of security can be done using SMS text, a phone call, an authenticator app, or a secure token.

Make sure to follow these steps to complete your Digital Identity setup smoothly!



FAQs

1. Why is Parkside making this change?
This upgrade will replace the existing multi-factor authentication service with a more robust and scalable platform, offering enhanced functionality and greater flexibility for future expansion

2. What must be done to prepare for this change?
Please be on the lookout for an email from the Treasury Management Platform, scheduled to arrive on February 5, 2025, to initiate the process. **Kindly note that the link provided in the email will be valid for only 7 days. Additionally, once the link is clicked, you will have 45 minutes to complete the process.**

3. Who do I contact if I have additional questions about this upgrade?
Please contact the Treasury Management Team at treasurymanagement@pfbt.com or send a secure message within the Treasury Portal.

4. Will I still need to use my token when initiating an ACH or Wire Payment?
There will be no changes to the payment processes. You will still be required to enter your token code along with your 4-digit PIN.

5. Can I use my current user ID?
Usernames must now be unique across all of our online banking platforms. In certain cases, you may be required to select a new User ID. We recommend using a combination of your current username and Treasury Company ID to ensure the User ID remains both unique and familiar.

6. 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 (,).

7. 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.

8. Can I use the “Don’t ask for codes again while using this browser” feature?
Yes, the 'Remember This Browser' feature is associated with the browser used during the 2FA setup. In the event of a brute-force attack or login attempt from an unrecognized browser, 2FA will require additional validation. Access will only be granted once successful verification is completed through the established 2FA methods.