



Create Digital and Configure Digital

Forgot Password

June 2026

Forgot Password

© 2026 Fiserv, Inc. or its affiliates. This work is confidential and its use is strictly limited. Use is permitted only in accordance with the terms of the agreement under which it was furnished. Any other use, duplication, or dissemination without the prior written consent of Fiserv, Inc. or its affiliates is strictly prohibited. The information contained herein is subject to change without notice. Except as specified by the agreement under which the materials are furnished, Fiserv, Inc. and its affiliates do not accept any liabilities with respect to the information contained herein and are not responsible for any direct, indirect, special, consequential or exemplary damages resulting from the use of this information. No warranties, either express or implied, are granted or extended by this document.

<http://www.fiserv.com>

Fiserv is a registered trademark of Fiserv, Inc.

Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

Purpose

This learning guide provides detailed instructions on how to navigate the Forgot Password process. To complement this guide, a Forgot Password video and job aid are available on Xchange.

Contents

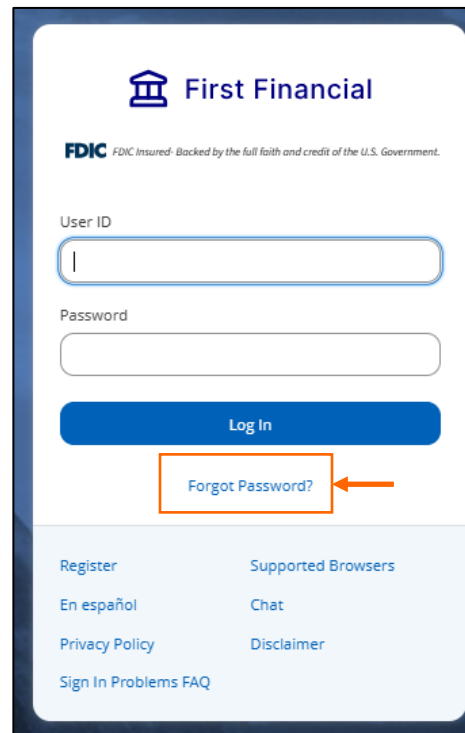
Accessing the Forgot Password Page	4
Entering Required Data for Identification	4
Identification Scoring System	6
Unsuccessful Sign-on	7
Required Fields missing	7
Optional Fields Missing	8
Successful Sign-on	9
Reset Password	10
Key Points to Remember	12

Accessing the Forgot Password Page

To ensure that users start the *Forgot Password* process from a trusted source, your financial institution's IT team or digital product managers should tether the password reset page directly to the institution's main website to reduce confusion and security risks. The URL should also open Create or Configure Digital in a new browser tab. The *Forgot Password* link should be on the sign-in page.

To access the *Forgot Password* process, the user should:

1. Select the *Forgot Password* link located on the online banking Sign-on Page.



Entering Required Data for Identification

After selecting the *Forgot Password* link, the user will be directed to a page that contains several fields to fill in. This allows the system to match data entered to the data on the core banking system to confirm identification.

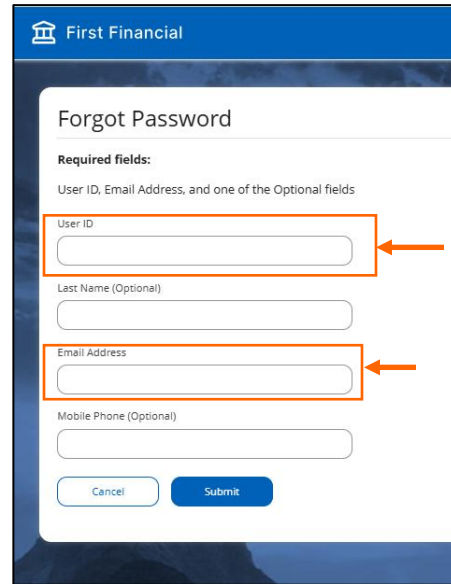
The user should follow the steps below to enter the required data to identify themselves. :

Forgot Password

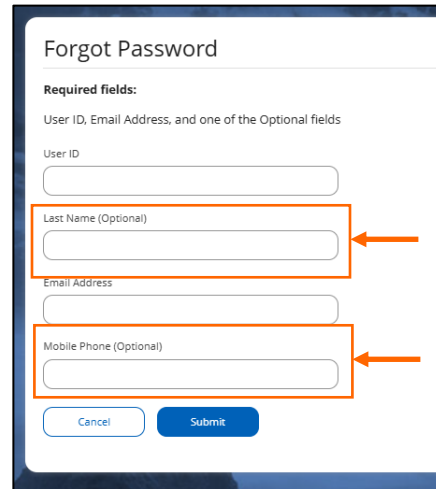


Required fields must be an exact match to information held in the systems of record.

1. The user completes the required fields:
 - a. *Online Banking User ID* – Matched to the Create or Configure Digital database
 - b. *Email Address* – Matched to the core

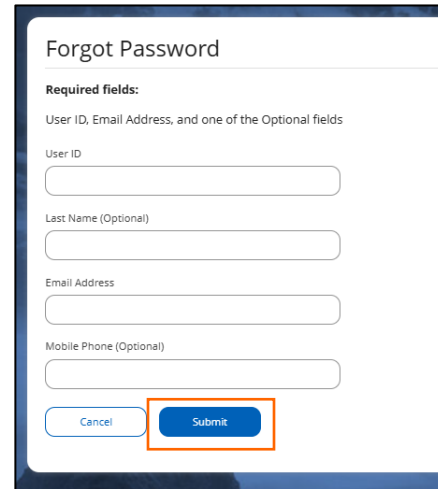


2. The user completes at least one of the optional fields:
 - a. *Last Name*
 - b. *Mobile Phone Number*



Forgot Password

3. Select *Search*.



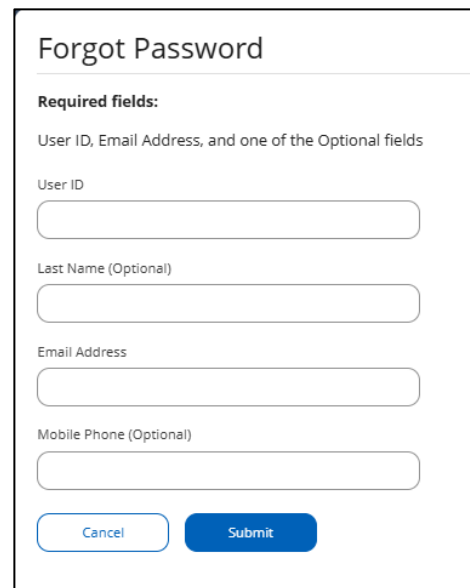
Identification Scoring System

All fields on the screen have a weighted score. The user must achieve an accumulated threshold score based on information in the fields matching correctly. The score is based on how difficult the data is to obtain if you are not the owner of the data.



All fields on the screen have a weighted score. The user must achieve an accumulated threshold score based on information in the fields matching correctly.

1. The configuration requires:
 - a. 100% match on all required fields
 - b. A match on at least one of the optional fields
 - c. Acceptable score from the system



Forgot Password

Unsuccessful Sign-on

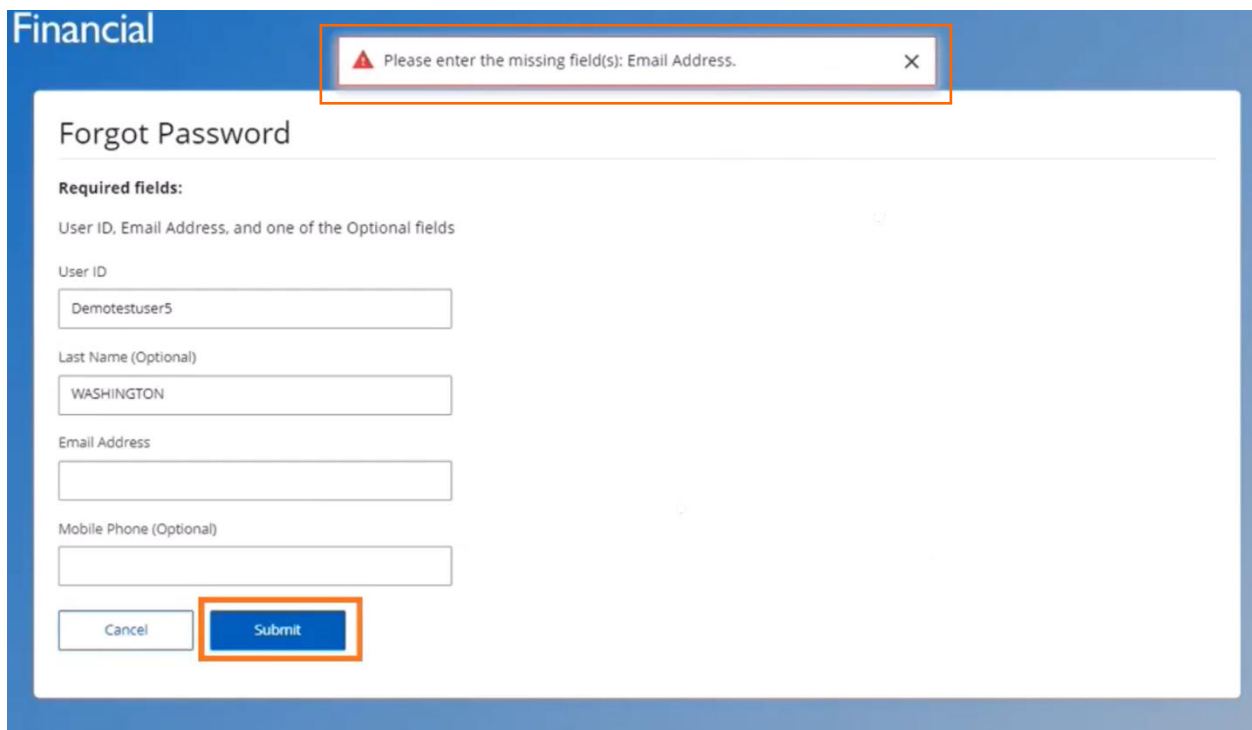
When a user enters incorrect data, the system will return an error message.

Required Fields missing

If required fields are missing, the error message may request data for the specific missing field.



Example: The user completes the user ID and Last Name fields and leaves the *Email Address* field blank. The system returns a message requesting the specific missing field.



The screenshot shows a web interface for a 'Financial' system. At the top, there is a blue header bar with the word 'Financial' in white. Below the header, a white box contains the title 'Forgot Password'. Inside this box, there is a section for 'Required fields:' which lists 'User ID, Email Address, and one of the Optional fields'. Below this list are four input fields: 'User ID' (containing 'Demotestuser5'), 'Last Name (Optional)' (containing 'WASHINGTON'), 'Email Address' (empty), and 'Mobile Phone (Optional)' (empty). At the bottom of the form are two buttons: 'Cancel' and 'Submit'. The 'Submit' button is highlighted with an orange border. Above the form, a red error message box is displayed, stating 'Please enter the missing field(s): Email Address.' with a close button (X) in the top right corner. The error message box is also highlighted with an orange border.

Forgot Password

Optional Fields Missing

When the user completes the user ID and Email fields but does not enter any optional fields, the system returns a message; “We were unable to validate your information. Ensure the information you have entered is accurate

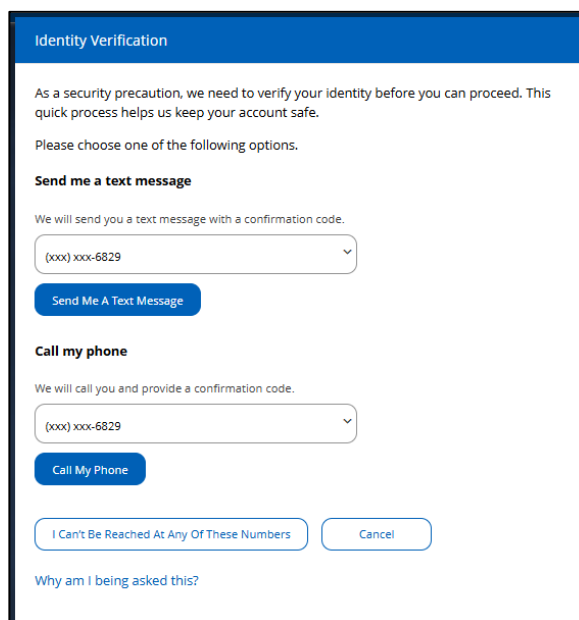
Note: The error message is deliberately vague to prevent an unauthorized person from knowing what information was not validated. In this case, the accumulated score is not enough because only two required data fields were completed.

The screenshot shows a web interface for the 'Forgot Password' process. At the top left, the word 'Financial' is displayed in a blue header. A red error message box is positioned at the top center, stating: 'We were unable to validate your information. Ensure the information you have entered is accurate.' Below this, the 'Forgot Password' title is centered. Under the heading 'Required fields:', a sub-instruction reads: 'User ID, Email Address, and one of the Optional fields'. The form contains four input fields: 'User ID' (with the text 'Demotestuser5'), 'Last Name (Optional)', 'Email Address' (with the text 'jhuibert@fiserv.com'), and 'Mobile Phone (Optional)'. At the bottom of the form are two buttons: 'Cancel' and 'Submit'.

Successful Sign-on

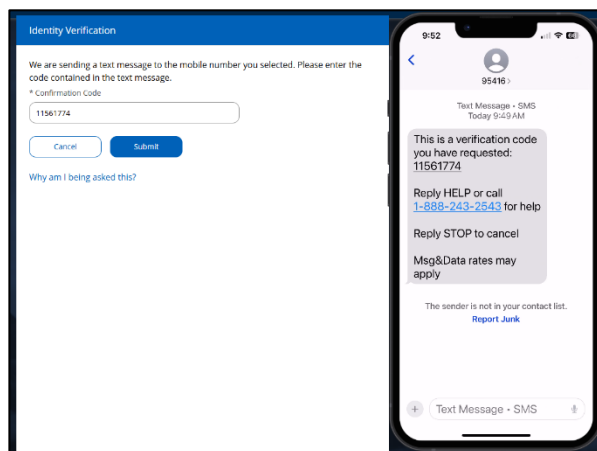
When the three data fields are completed and verified correctly, the score value exceeds the threshold limit to pass. The user will be presented with the second level of security, the SecureNow One Time PIN (OTP) challenge.

1.
 - a. The SecureNow One-Time PIN (OTP) Challenge displays
 - b. The user chooses how they want to receive their PIN:
 1. Text Message
 2. Phone Call (Voice Call)
 - c. The user must have access to the phone number they select from the drop-down menu
 - d. If the user is not able to access any of the listed phone numbers, they should select the *I Can't Be Reached At Any Of These Numbers* to return to the Online Banking Login page



2. The user enters the PIN received by text or call on their phone in the *Confirmation Code* field of the *Identity Verification* page

Select *Submit*



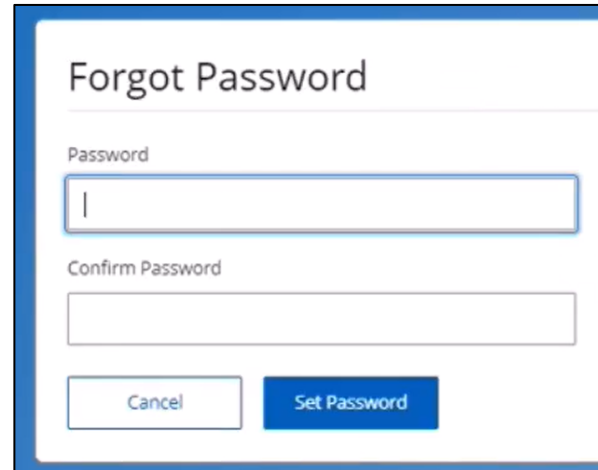
For One-Time PIN authentication, financial institutions should test both text and phone methods to ensure that they work correctly.

Forgot Password

Reset Password

When the One-Time PIN code is verified, the user is directed to the password reset screen.

1. The user follows the prompts to set a new password

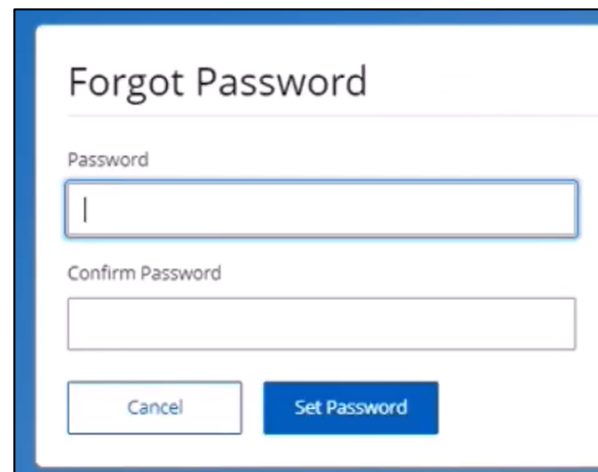


The screenshot shows a web form titled "Forgot Password". It contains two input fields: "Password" and "Confirm Password". The "Password" field has a blue border and a cursor. Below the fields are two buttons: "Cancel" and "Set Password".

2. The password must meet the requirements:
 - a. 12-32 characters long
 - b. At least one lower case letter
 - c. At least one uppercase letter
 - d. At least one number

Confirm the Password

Select *Set Password*

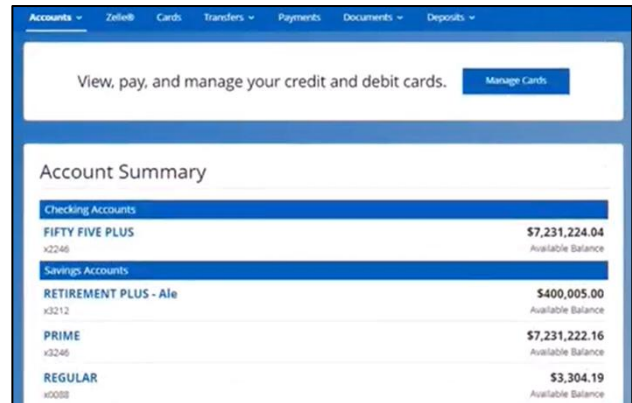


This is a duplicate of the first screenshot, showing the "Forgot Password" form with "Password" and "Confirm Password" fields, and "Cancel" and "Set Password" buttons.

Forgot Password

3. When the user's password has been reset successfully, the Account Summary page displays.

Note: If the user's account is locked due to too many failed login attempts, going through the forgot password process will automatically unlock the account.



The screenshot shows the 'Account Summary' page in the Fiserv portal. At the top, there is a navigation bar with links for Accounts, Zelle, Cards, Transfers, Payments, Documents, and Deposits. Below the navigation bar, a message states 'View, pay, and manage your credit and debit cards.' with a 'Manage Cards' button. The main content area is titled 'Account Summary' and lists the user's accounts. The accounts are categorized into 'Checking Accounts' and 'Savings Accounts'. The 'Checking Accounts' section includes 'FIFTY FIVE PLUS' with an available balance of \$7,231,224.04. The 'Savings Accounts' section includes 'RETIREMENT PLUS - Ale' with an available balance of \$400,005.00, 'PRIME' with an available balance of \$7,231,222.16, and 'REGULAR' with an available balance of \$3,304.19.

Account Summary	
Checking Accounts	
FIFTY FIVE PLUS x2246	\$7,231,224.04 Available Balance
Savings Accounts	
RETIREMENT PLUS - Ale x3212	\$400,005.00 Available Balance
PRIME x3246	\$7,231,222.16 Available Balance
REGULAR x0008	\$3,304.19 Available Balance

Key Points to Remember



Required fields must be an exact match to information held in the systems of record.



All fields on the screen have a weighted score. The user must achieve an accumulated threshold score based on information in the fields matching correctly.



For One-Time PIN authentication, financial institutions should test both text and phone methods to ensure that they work correctly.



Fiserv Corporate Headquarters
600 N. Vel R. Phillips Avenue
Milwaukee, Wisconsin 53203
United States
Phone: 800-872-7882
Fax: 262-879-5013
www.fiserv.com

© 2025 Fiserv, Inc. or its affiliates. Fiserv is a trademark of Fiserv, Inc., registered or used in the United States and foreign countries, and may or may not be registered in your country. All trademarks, service marks, and trade names referenced in this material are the property of their respective owners.