

# Oracle® Banking Digital Experience Cloud Service

## Small & Medium Business PIN / Pattern / Touch and Face Authentication User Manual



Release 25.1.1.0.0

G46565-01

October 2025

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

G46565-01

Copyright © 2015, 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

Purpose	i
Audience	i
Documentation Accessibility	i
Diversity and Inclusion	i
Conventions	ii
Related Resources	ii
Screenshot Disclaimer	ii
Acronyms and Abbreviations	ii
Basic Actions	ii
Symbols and Icons	iii

## 1 Pattern / PIN Authentication

---

1.1	Pattern Based Authentication	1
1.1.1	Set Pattern (First Time Login Flow)	1
1.1.2	Manage Pattern	11
1.1.3	Login using pattern	13
1.2	PIN based Authentication	15
1.2.1	Set PIN (First Time Login Flow)	15
1.2.2	Manage PIN	25
1.2.3	Login using PIN	27
1.3	Face ID Based Authentication	29
1.3.1	Face ID Based- Set Face Recognition (First Time Login Flow)	29
1.3.2	Login using Face ID	37
1.4	Touch ID Based Authentication	39
1.4.1	Touch ID Recognition (First Time Login)	39
1.4.2	Login using Touch ID	45

## 2 Using Alternate Login Method

---

### 3 FAQ

---

#### Index

---

# Preface

- [Purpose](#)
- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Conventions](#)
- [Related Resources](#)
- [Screenshot Disclaimer](#)
- [Acronyms and Abbreviations](#)
- [Basic Actions](#)
- [Symbols and Icons](#)

## Purpose

This guide is designed to help acquaint you with the Oracle Banking application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

## Audience

This document is intended for the following audience:

- Customers
- Partners

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### **Access to Oracle Support**

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

## Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to

build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

## Related Resources

For more information on any related features, refer to the following documents:

- Oracle Banking Digital Experience Installation Manuals
- Oracle Banking Digital Experience Licensing Manuals

## Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

## Acronyms and Abbreviations

The list of the acronyms and abbreviations used in this guide are as follows:

**Table 1 Acronyms and Abbreviations**

Abbreviation	Description
OBDX	Oracle Banking Digital Experience

## Basic Actions

Most of the screens contain icons to perform all or a few of the basic actions. The actions which are called here are generic, and it varies based on the usage and the applicability. The table below gives a snapshot of them:










**Table 2 Basic Actions and Descriptions**

Action	Description
<b>Back</b>	In case you missed to specify or need to modify the details in the previous segment, click <b>Back</b> to navigate to the previous segment.
<b>Cancel</b>	Click <b>Cancel</b> to cancel the operation input midway without saving any data. You will be alerted that the input data would be lost before confirming the cancellation.
<b>Next</b>	On completion of input of all parameters, click <b>Next</b> to navigate to the next segment.
<b>Save</b>	On completion of input of all parameters, click <b>Save</b> to save the details.
<b>Save &amp; Close</b>	Click <b>Save &amp; Close</b> to save the data captured. The saved data will be available in <b>View Business Product</b> with <i>In Progress</i> status. You can work on it later by picking it from the <b>View Business Product</b> .
<b>Submit</b>	On completing the input of all parameters, click <b>Submit</b> to proceed with executing the transaction.
<b>Reset</b>	Click <b>Reset</b> to clear the data entered.
<b>Refresh</b>	Click <b>Refresh</b> to update the transaction with the recently entered data.
<b>Download</b>	Click <b>Download</b> to download the records in PDF or XLS format.


## Symbols and Icons

The following are the symbols/icons you are likely to find in this guide:

**Table 3 Symbols and Icons**

Symbols and Icons	Description
	Add data segment
	Close
	Maximize
	Minimize
	Open a list
	Open calendar
	Perform search
	View options
	View records in a card format for better visual representation.

**Table 3 (Cont.) Symbols and Icons**

Symbols and Icons	Description
	View records in tabular format for better visual representation.



# 1

## Pattern / PIN Authentication

- [Pattern Based Authentication](#)
- [PIN based Authentication](#)
- [Face ID Based Authentication](#)
- [Touch ID Based Authentication](#)

### 1.1 Pattern Based Authentication

Pattern based authentication allows a user to login to Futura Bank mobile application by drawing a pattern on the screen instead of entering their user ID and password. The user can define a pattern for authentication and the same needs to be drawn every time for login and authentication.

#### Note

Pattern based authentication is available for Futura Bank application for Android and iOS platforms.

#### Features Supported In the Application

- [Set Pattern](#)
- [Manage Pattern](#)
- [Pattern Visibility](#)
- [Login using pattern](#)

#### Pre-Requisites

The user must download the **Futura Bank** application and should have a valid account with the bank with online banking enabled.

- [Set Pattern \(First Time Login Flow\)](#)
- [Manage Pattern](#)
- [Login using pattern](#)




#### 1.1.1 Set Pattern (First Time Login Flow)


The user can define a pattern for login using their Futura Bank login credentials from Futura Bank mobile application. The user can also define if the pattern has to be kept visible or invisible at the time of drawing the same for logging into the application.


##### To set a pattern for login:

1. Launch the **Futura Bank** application.  
The **Futura Bank** login page appears.

Figure 1-1 Futura Bank Login Page

10:32   

 **Futura Bank**



[Forgot Password / Username](#)

**Login**

**Quick Snapshot**

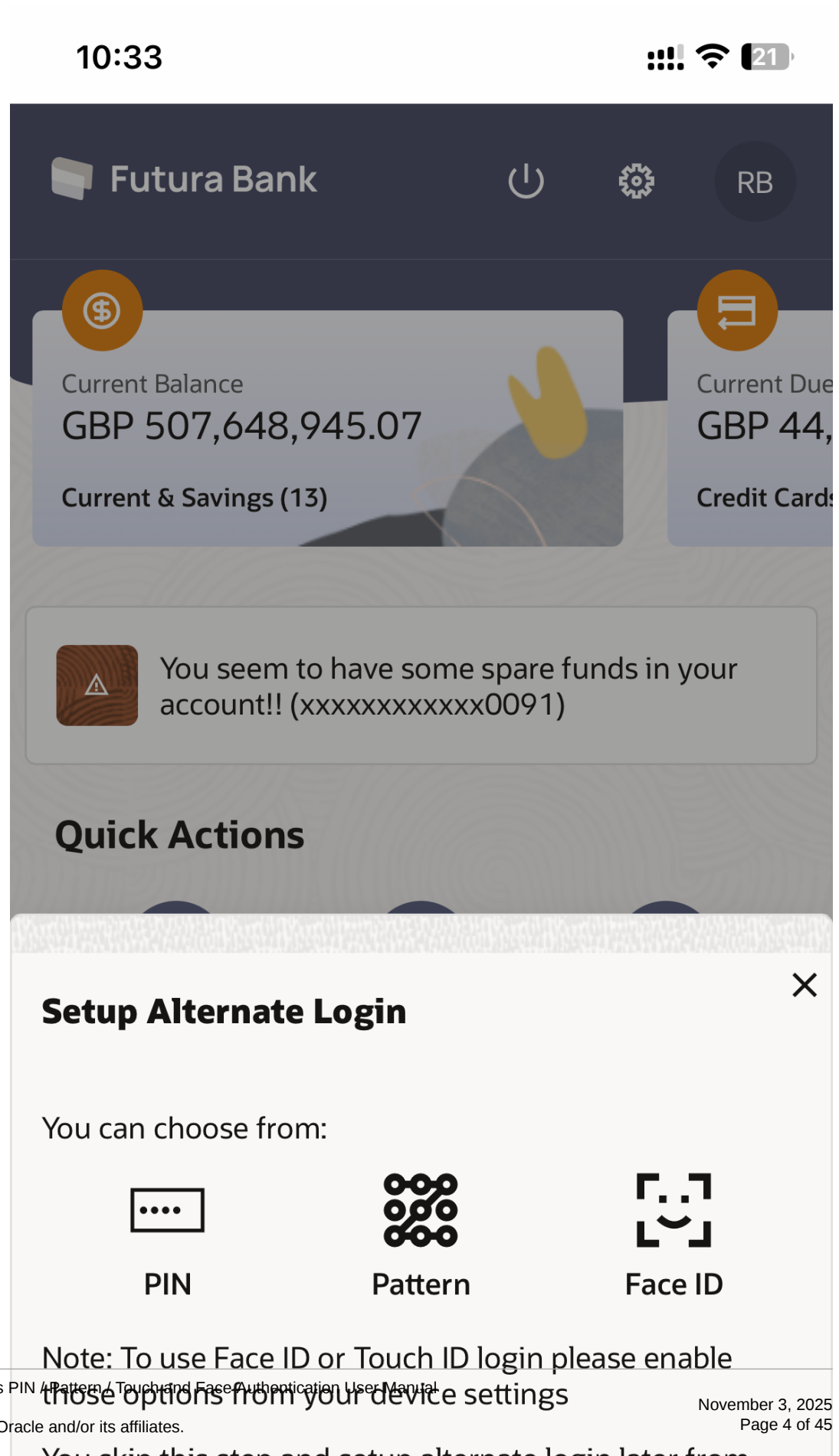
**Register**

[Copyright Statement](#)

2. In the **Username** field, enter the user ID.
3. In the **Password** field, enter the password.
4. Click **Login**.

The dashboard with **Select Alternate Login Method** popup screen appears.

Figure 1-2 Select Alternate Login Method screen- Pattern



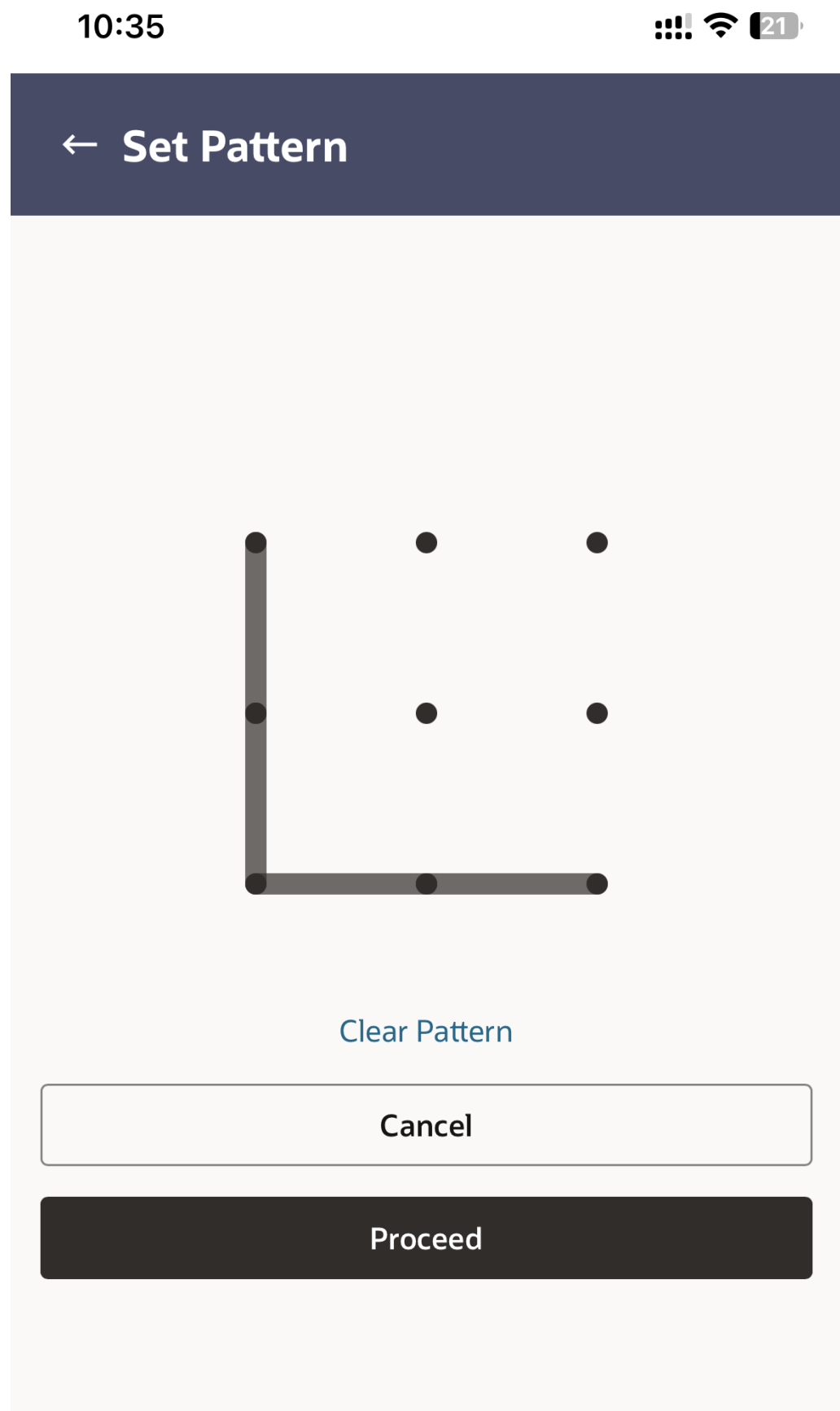
**Note**

- a. : For registering **Alternate Login Method** on the User's device will automatically cancel the previous active registrations if any on other devices. Application verify user with unique identifier linked to device.
- b. User can click **Setup Later** and skipped and set later by navigating from the **Profile** → **Settings**. Refer **Manage Pattern** section for more information.

5. Select the **Pattern** option as the login method.

The **Set Pattern** screen appears.

Figure 1-3 Set Pattern screen



6. Set the desired pattern. Draw a pattern connecting a minimum of 4 dots.
7. Click **Proceed** to proceed to next step.

The **Confirm Pattern** screen appears.

OR

Click **Cancel** to cancel the transaction.

OR

Click **Clear Pattern** to reset the pattern and redraw it.

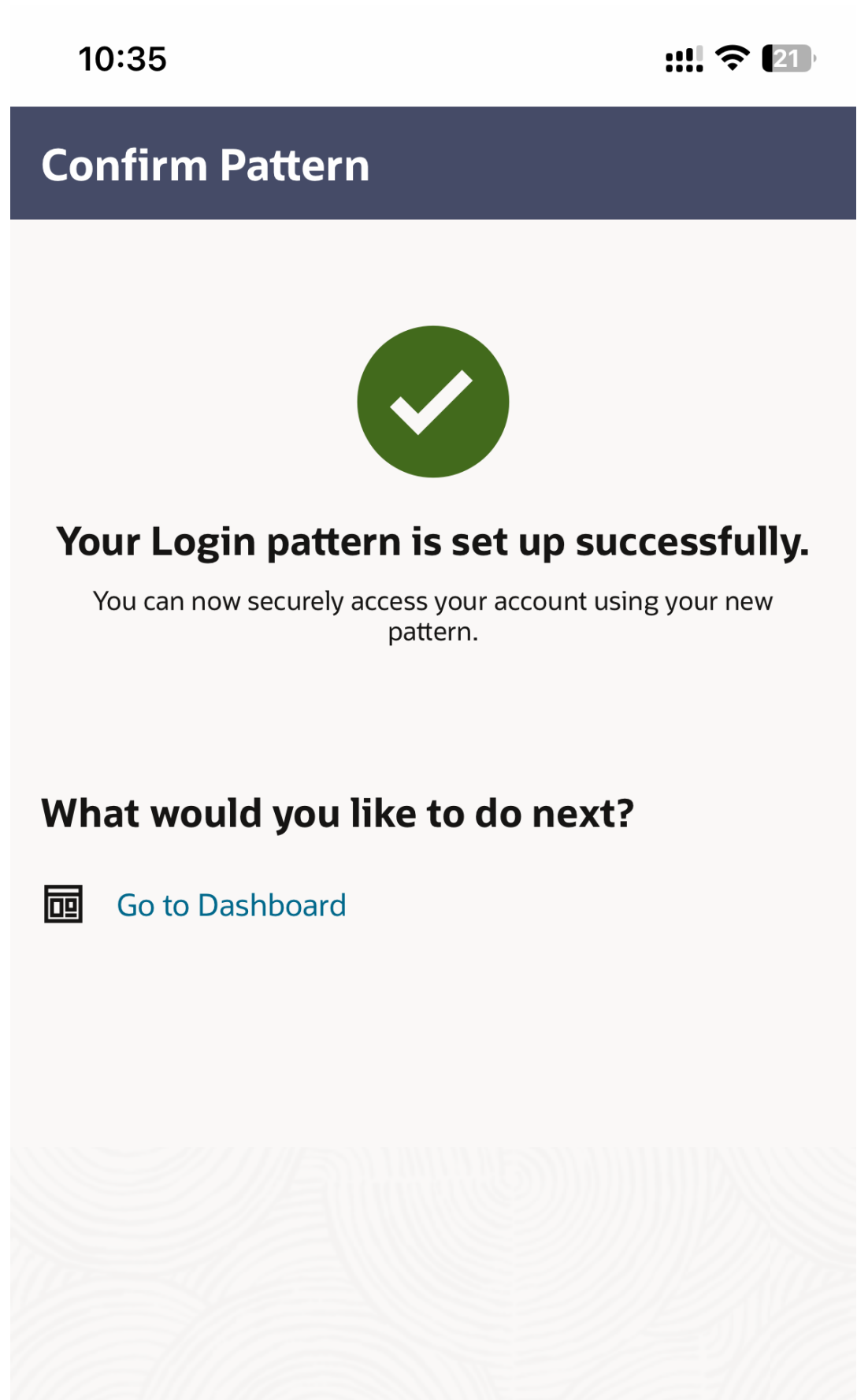
Figure 1-4 Confirm Pattern screen





8. Redraw the same pattern to confirm the pattern.
9. Toggle the **Pattern Visibility** button to show/hide the pattern during login.
10. Click **Confirm**.  
OR  
Click **Cancel** to cancel the transaction.
11. The success message of pattern set appears.

Figure 1-5 Success Message screen



**Note**

Once the pattern is set, the system will prompt you to draw the pattern at the time of login.

## 1.1.2 Manage Pattern

Using this option, the user can change or reset the login pattern defined.

In case the user wants to change the alternate login from Pattern to any other method (for example from PIN to Pattern) or if it has got locked due to maximum number of incorrect attempts being reached, the user can reset it using this option.

**To reset the pattern for login transaction:**

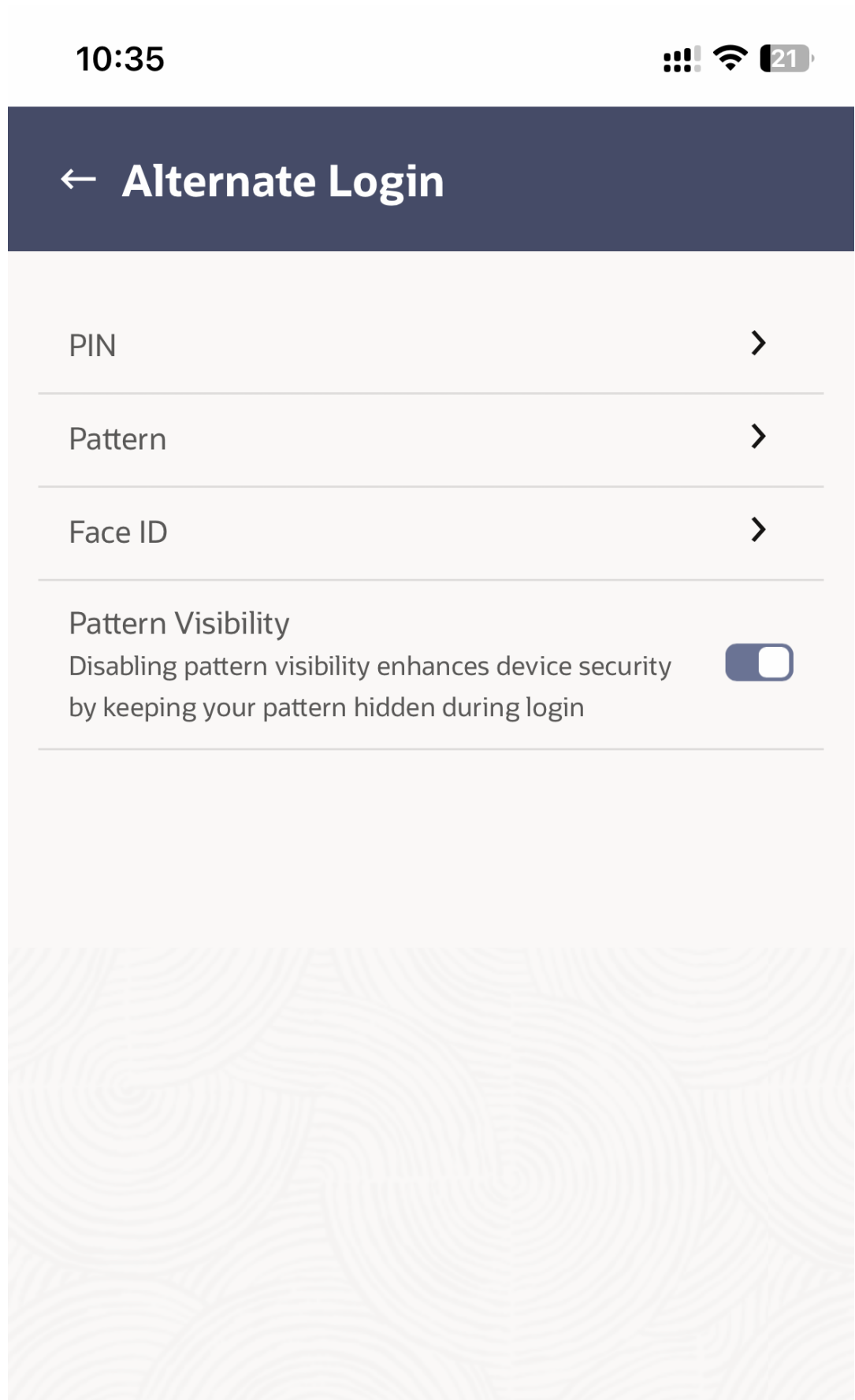
1. Login to the **Futura Bank** application.
2. From the toggle menu, click **My Preferences**, click **Password & Security**, and then click on the **Alternate Login – Pattern** option.

The **Verify User** screen appears.

3. In the **Enter Password** field, enter the password.
4. Click **Proceed**.

The **Alternate Login** screen appears.

Figure 1-6 Manage Pattern &amp; Pattern Visibility



5. Toggle the **Pattern Visibility** button to show/hide the pattern during login.

Next time you draw the pattern at the time of login, you will be able to see it on the screen.

**Note**

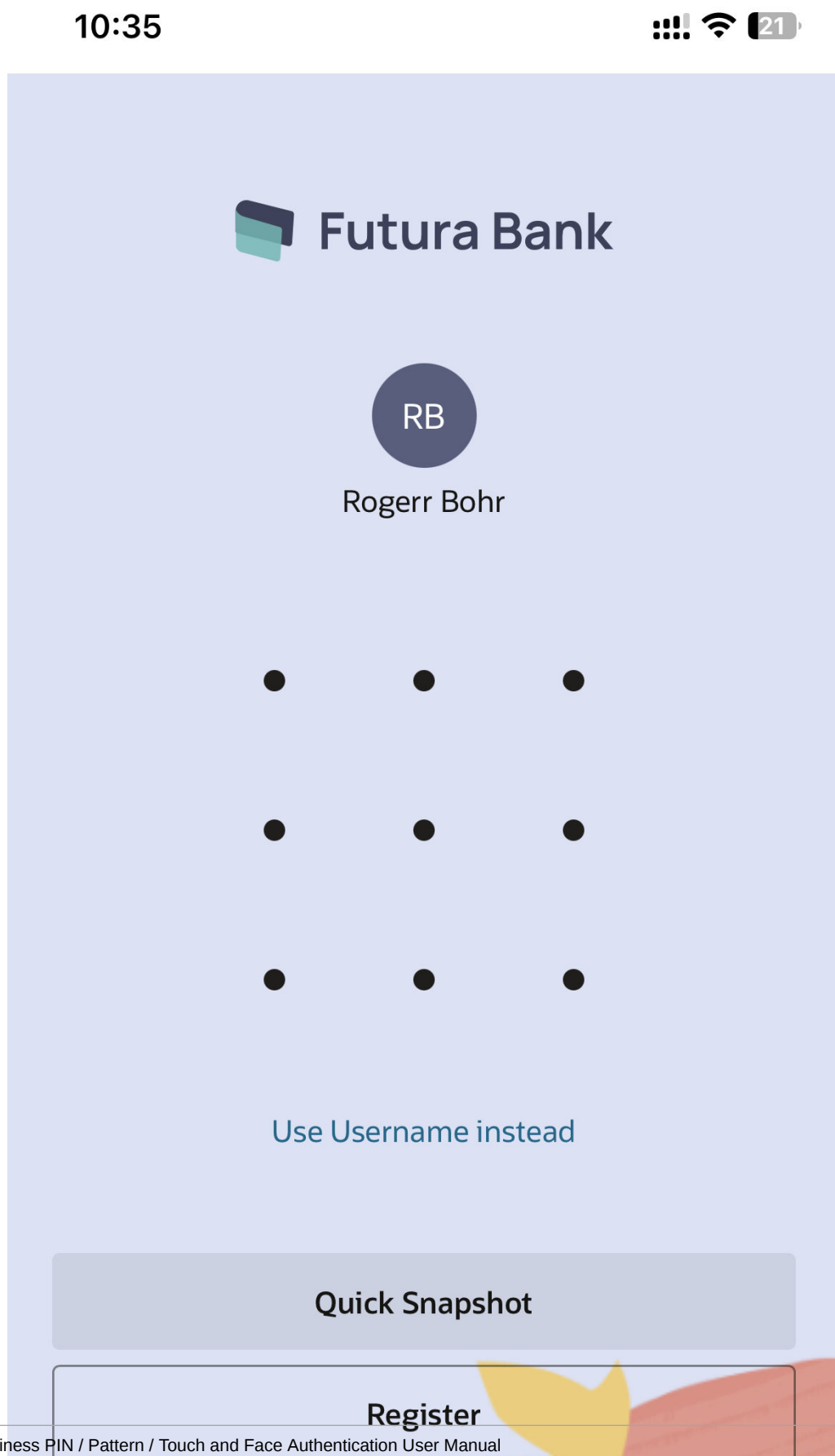
By default, the **Pattern Visibility** option is disabled. If you keep the pattern visibility as disabled, you will not be able to see the pattern that you are drawing at the time of login and this will prevent any unauthorized access to the application.

6. Click **Pattern** to update the pattern.  
The **Set Pattern** screen appears.
7. Draw a pattern connecting a minimum of 4 dots.  
The **Confirm Pattern** screen appears.
8. Redraw the same pattern for confirmation.
9. Click **Confirm**. The **Confirm Pattern** screen appears.  
OR  
Click **Cancel** to cancel the transaction.
10. The success message for new pattern being set is displayed.  
Click **Go to Dashboard**, to navigate to the Dashboard.  
OR  
Click **More Security Options** to go to other security options.

### 1.1.3 Login using pattern

This feature allows a user to login to Futura Bank mobile application by drawing a pattern on the screen instead of entering their user ID and password after setting the pattern as alternate login.

Figure 1-7 Login Using pattern



**Note**

Click on the link **Use Username Instead** to log into application with user ID and password.

## 1.2 PIN based Authentication

This option allows the user to login to the Futura Bank application using a PIN instead of a user ID and password. The user can define a 4 or 6 digit numeric PIN for login. The user also has the option of resetting the PIN and changing the alternate login method from PIN to any other method. The user can also define if the pattern has to be kept visible or invisible at the time of drawing the same for logging into the application.

**Features Supported In the Application:**

- [Set PIN](#)
- [Manage PIN](#)
- [Login using PIN](#)
- [Set PIN \(First Time Login Flow\)](#)
- [Manage PIN](#)
- [Login using PIN](#)




### 1.2.1 Set PIN (First Time Login Flow)


The user can define a PIN for login on Futura Bank mobile application by entering the user ID and password.


**To set PIN for login transaction:**

1. Launch the **Futura Bank** application.  
The **Futura Bank** login page appears.

Figure 1-8 Futura Bank Login Page

10:32   

 **Futura Bank**



[Forgot Password / Username](#)

**Login**

**Quick Snapshot**

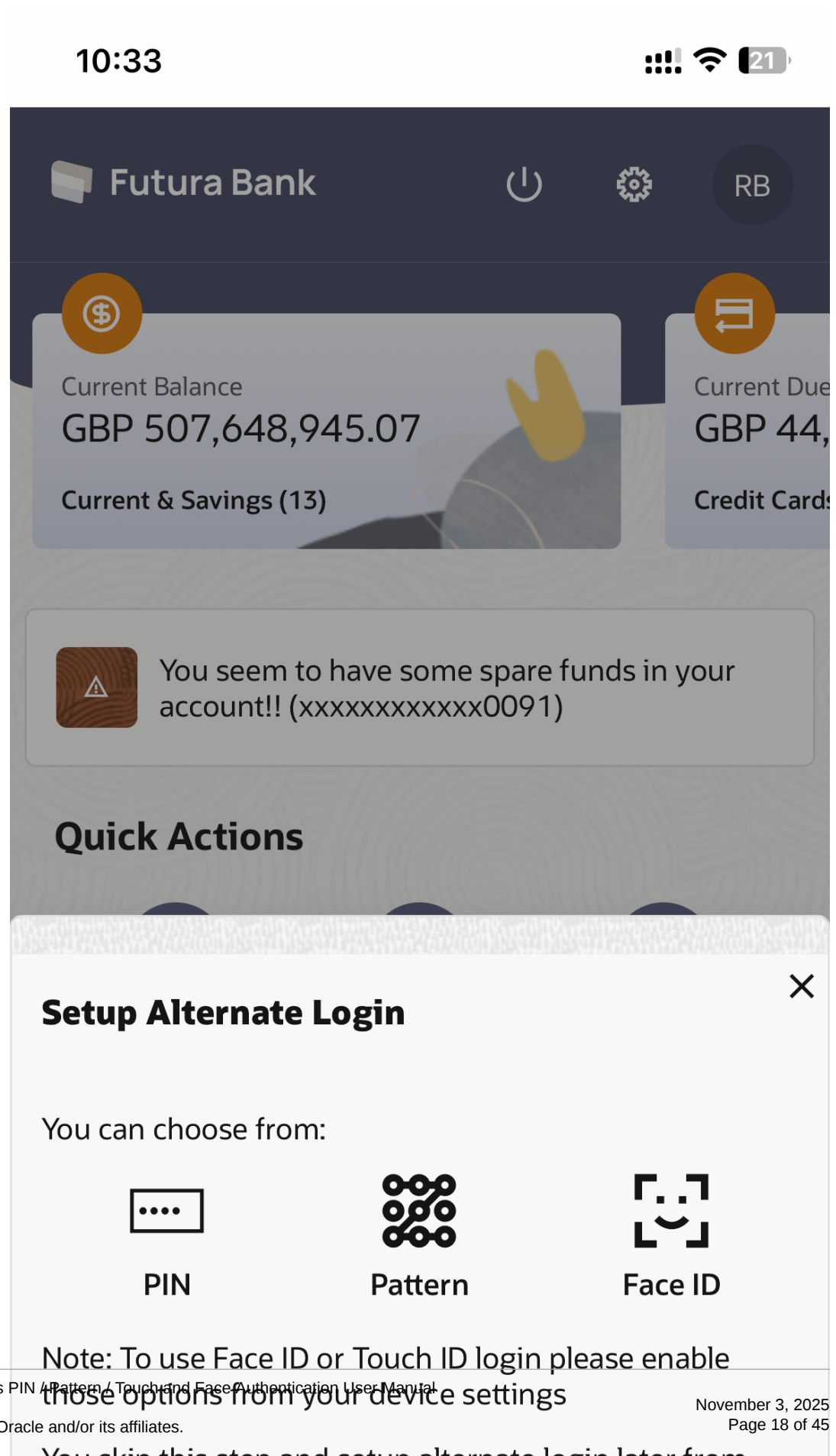
**Register**

[Copyright Statement](#)



2. In the **Username** field, enter the user ID.
3. In the **Password** field, enter the password.
4. Click **Login**.

Figure 1-9 Select Alternate Login Method screen- PIN



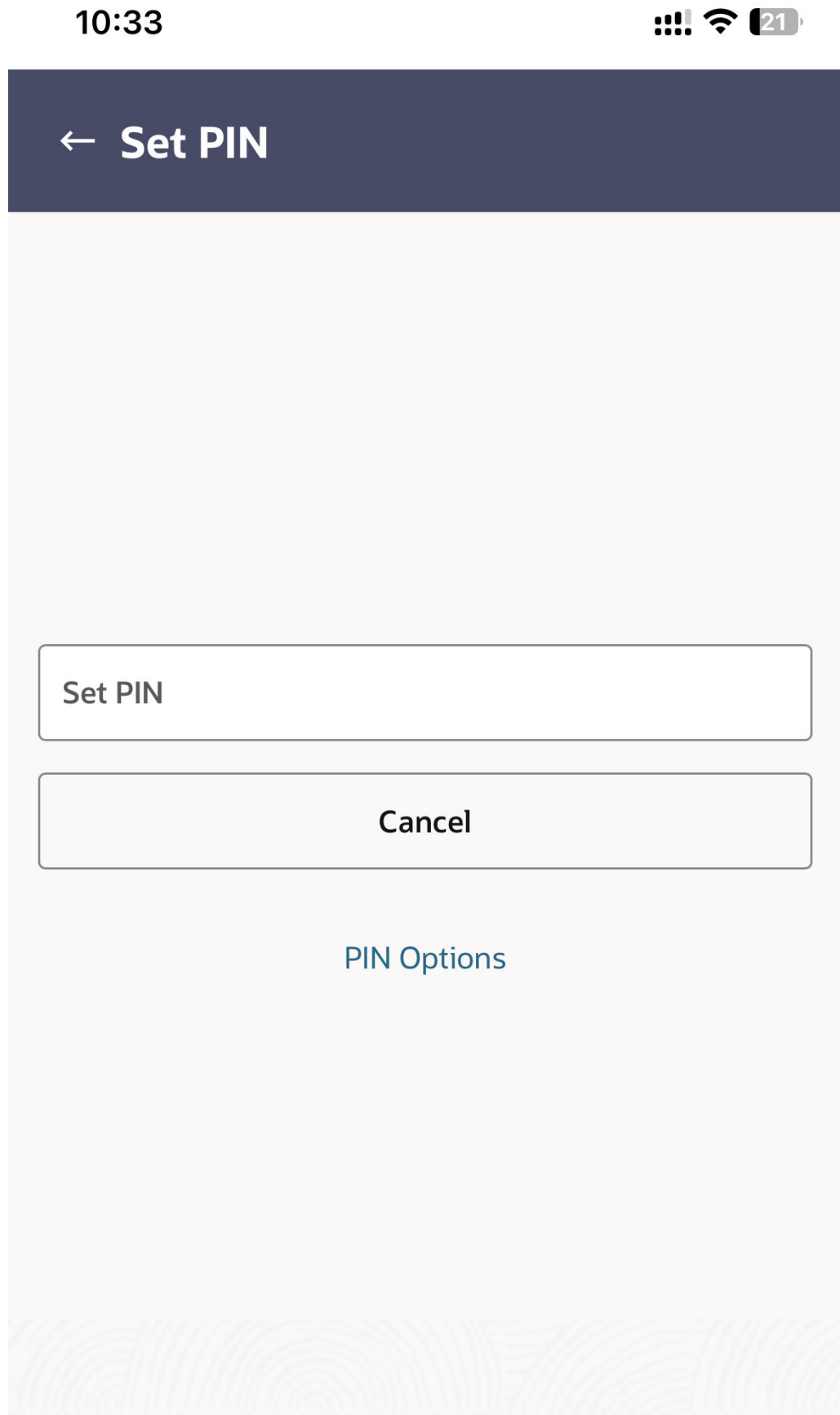
**Note**

- a. For registering **Alternate Login Method** on the User's device will automatically cancel the previous active registrations if any on other devices. Application verify user with unique identifier linked to device.
- b. User can click **Setup Later** and skipped and set later by navigating from the **Profile** → **Settings**. Refer **Manage PIN** section for more information.

5. Select the **PIN** based authentication method.

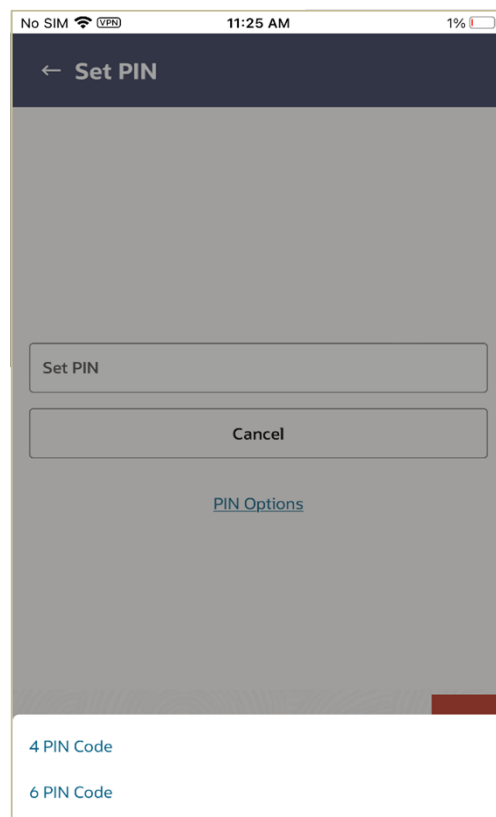
The **Set PIN** screen is displayed.

Figure 1-10 Set PIN screen



6. In the **Set PIN** field, enter the PIN that needs to be set for login.  
The **Confirm PIN** screen appears.  
OR  
Click **Cancel** to cancel the transaction.  
OR  
Click **PIN Options** to choose the pin length.
7. Click **Login**.  
The **Select Login Method** screen appears.

**Figure 1-11 PIN Options Screen**



- a. Select the desired PIN length.

**Table 1-1 Field Description**

Field Name	Description
<b>PIN Options</b>	This option lets the user to decide the length of the PIN. The options are: <ul style="list-style-type: none"><li>• 4 PIN Passcode: Set the 4 digit <b>PIN</b> for login transaction.</li><li>• 6 PIN Passcode: Set the 6 digit <b>PIN</b> for login transaction.</li></ul>

Figure 1-12 Confirm PIN screen

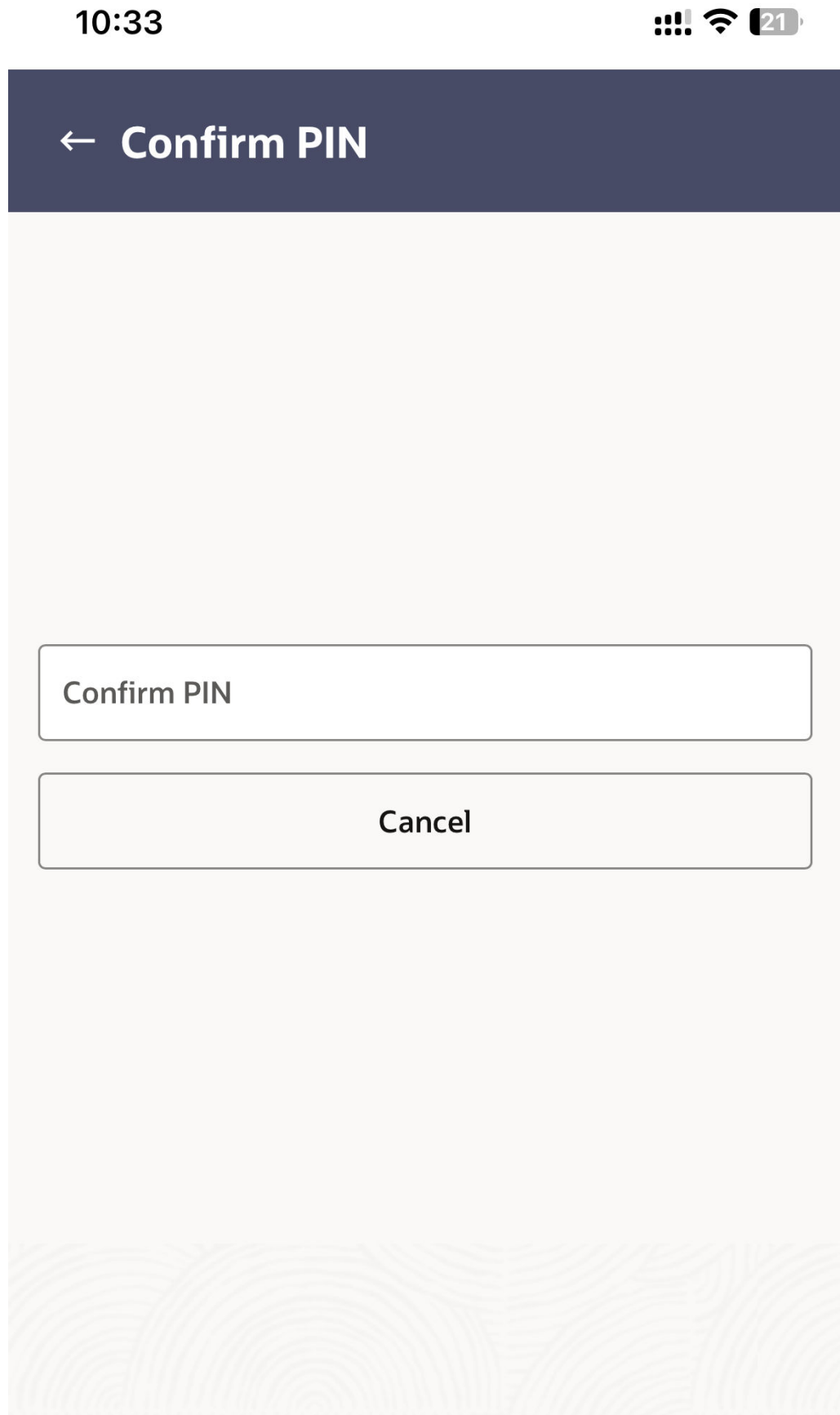
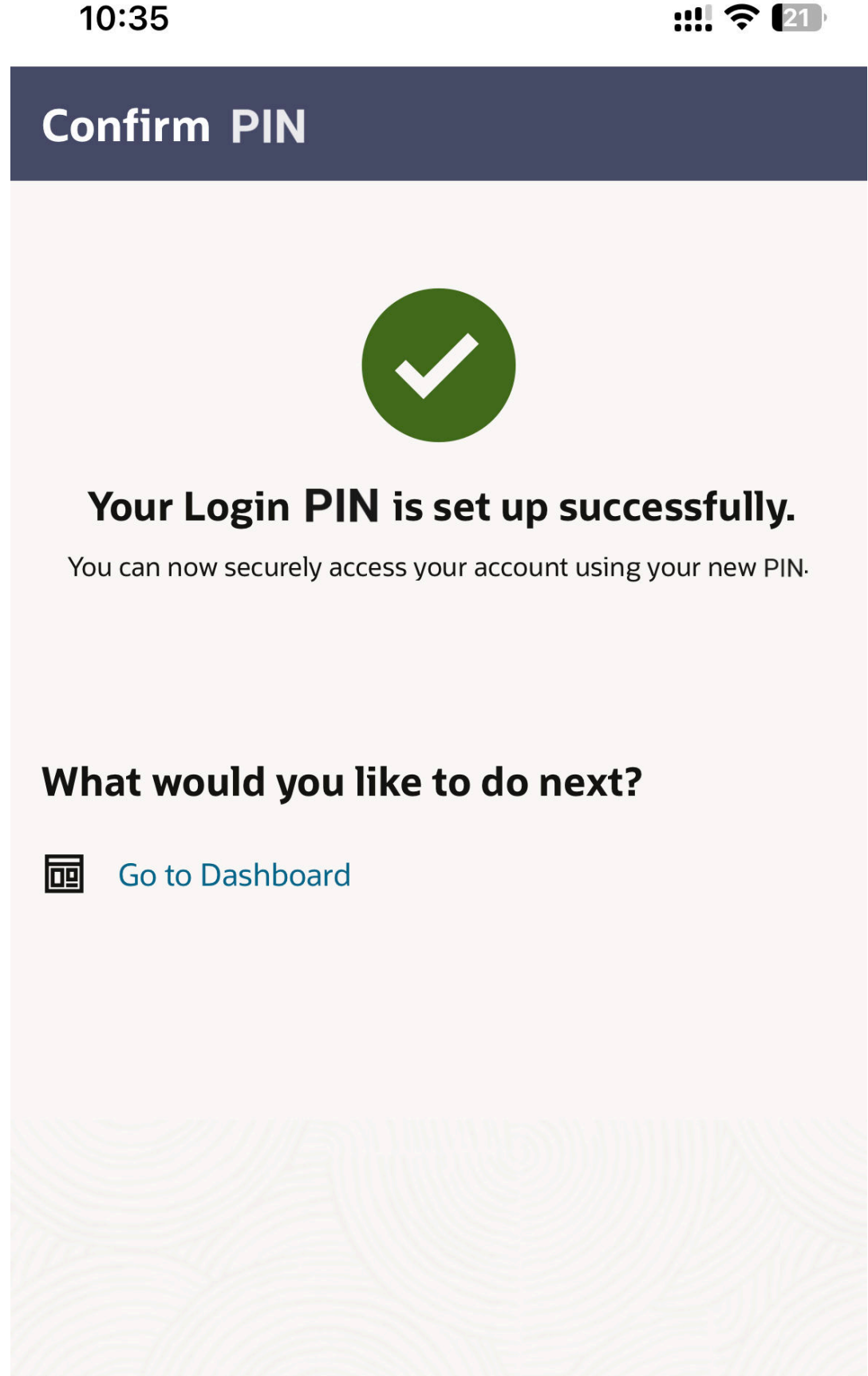


Table 1-2 Field Description

Field Name	Description
Confirm PIN	Re-enter the <b>PIN</b> to confirm.

8. In the **Confirm PIN** field, re-enter the pin for confirmation.  
OR  
Click **Cancel** to cancel the transaction.
9. The success message of PIN set appears.

Figure 1-13 Success Message screen





10. The PIN will get set and you will be redirected to the Dashboard.

**Note**

Once the PIN is set, the system will prompt you to enter the PIN at the time of login.

## 1.2.2 Manage PIN

Using this option the user can change or reset the login PIN defined.

In case the user wants to change the alternate login from PIN to any other method (for example from PIN to Pattern) or if it has got locked due to maximum number of incorrect PIN entries, the user can reset it using this option.

**To reset the PIN for login transaction:**

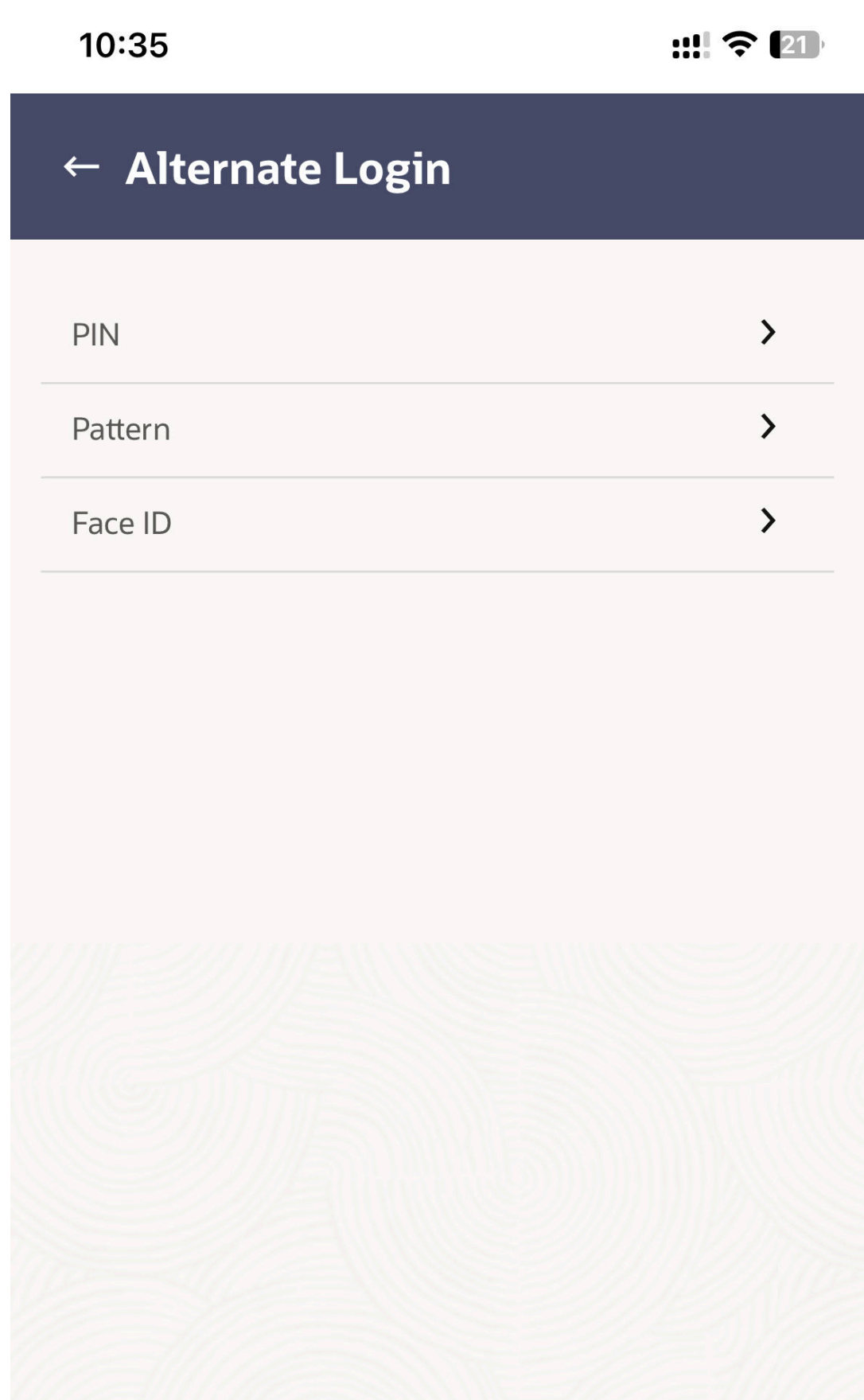
1. Login to the **Futura Bank** application.
2. From the toggle menu, click **My Preferences**, click **Password & Security**, and then click on the **Alternate Login – PIN** option.

The **Verify User** screen appears.

3. In the **Enter Password** field, enter the password.
4. Click **Proceed**.

The **Alternate Login** screen appears.

Figure 1-14 Manage PIN

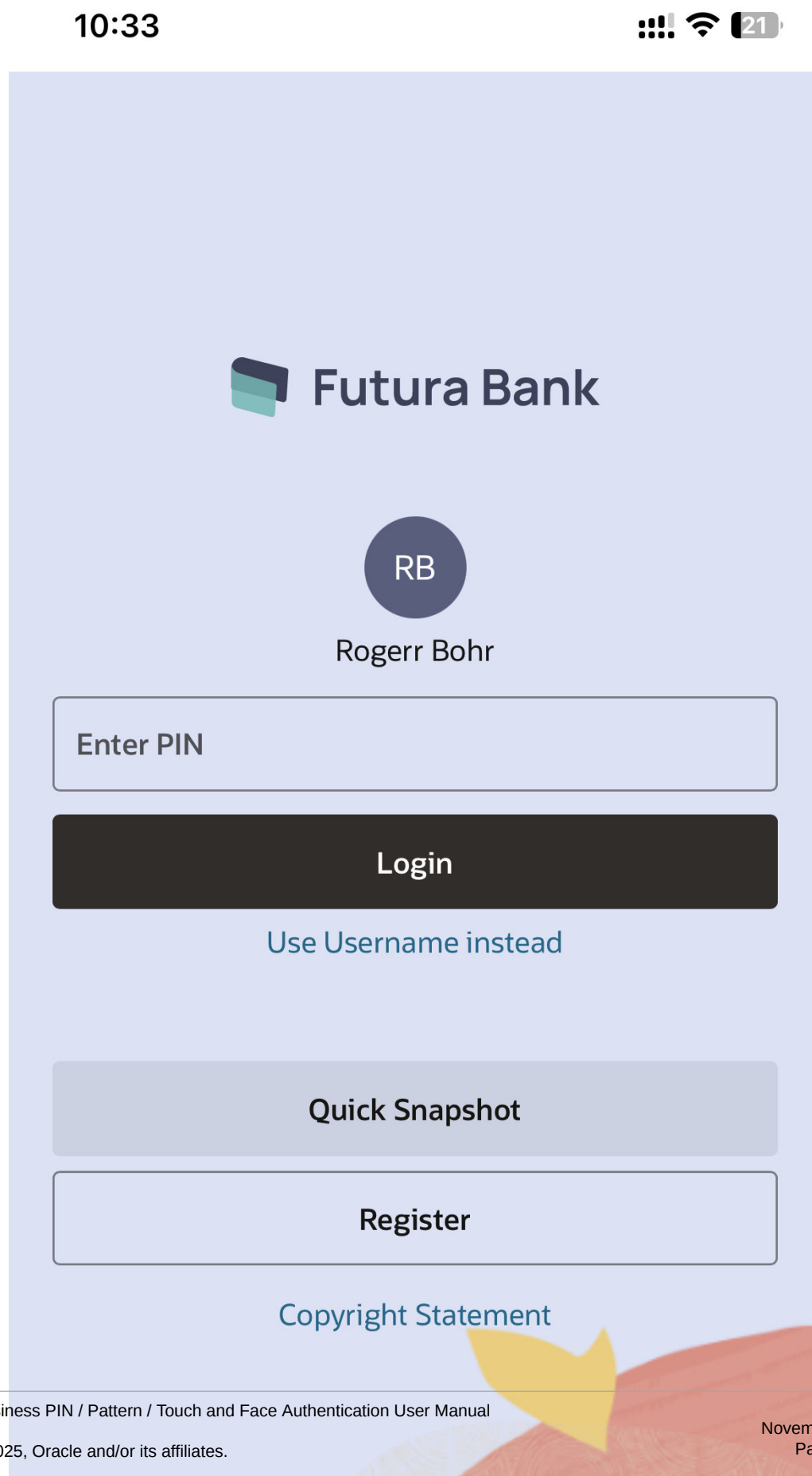


5. In the **Set PIN** field, enter PIN to be set for login.  
The **Confirm PIN** screen appears.
6. In the **Confirm PIN** field, re-enter the pin for confirmation.
7. The success message for new pattern being set is displayed.  
Click **Go to Dashboard**, to navigate to the Dashboard.  
OR  
Click **More Security Options** to go to other security options.

### 1.2.3 Login using PIN

This feature allows a user to login to Futura Bank mobile application by using PIN instead of entering their user ID and password after setting the PIN as alternate login.

Figure 1-15 Login Using PIN



**Note**

Click on the link **Use Username Instead** to log into application with user ID and password.

## 1.3 Face ID Based Authentication

This option allows the user to login to the Futura Bank application using Face ID instead of user ID and password. The user also has the option of changing their alternate login from Face ID to any other method.

**Features Supported In the Application:**

- [Set Face Recognition](#)
- [Login using Face ID](#)
- [Face ID Based- Set Face Recognition \(First Time Login Flow\)](#)
- [Login using Face ID](#)




### 1.3.1 Face ID Based- Set Face Recognition (First Time Login Flow)


The user can define Face ID for login on Futura Bank mobile application by entering the user ID and password.


**To set face recognition for login transaction:**

1. Launch the **Futura Bank** application.  
The **Futura Bank** login page appears.

Figure 1-16 Futura Bank login

10:32   

 **Futura Bank**



[Forgot Password / Username](#)

**Login**

**Quick Snapshot**

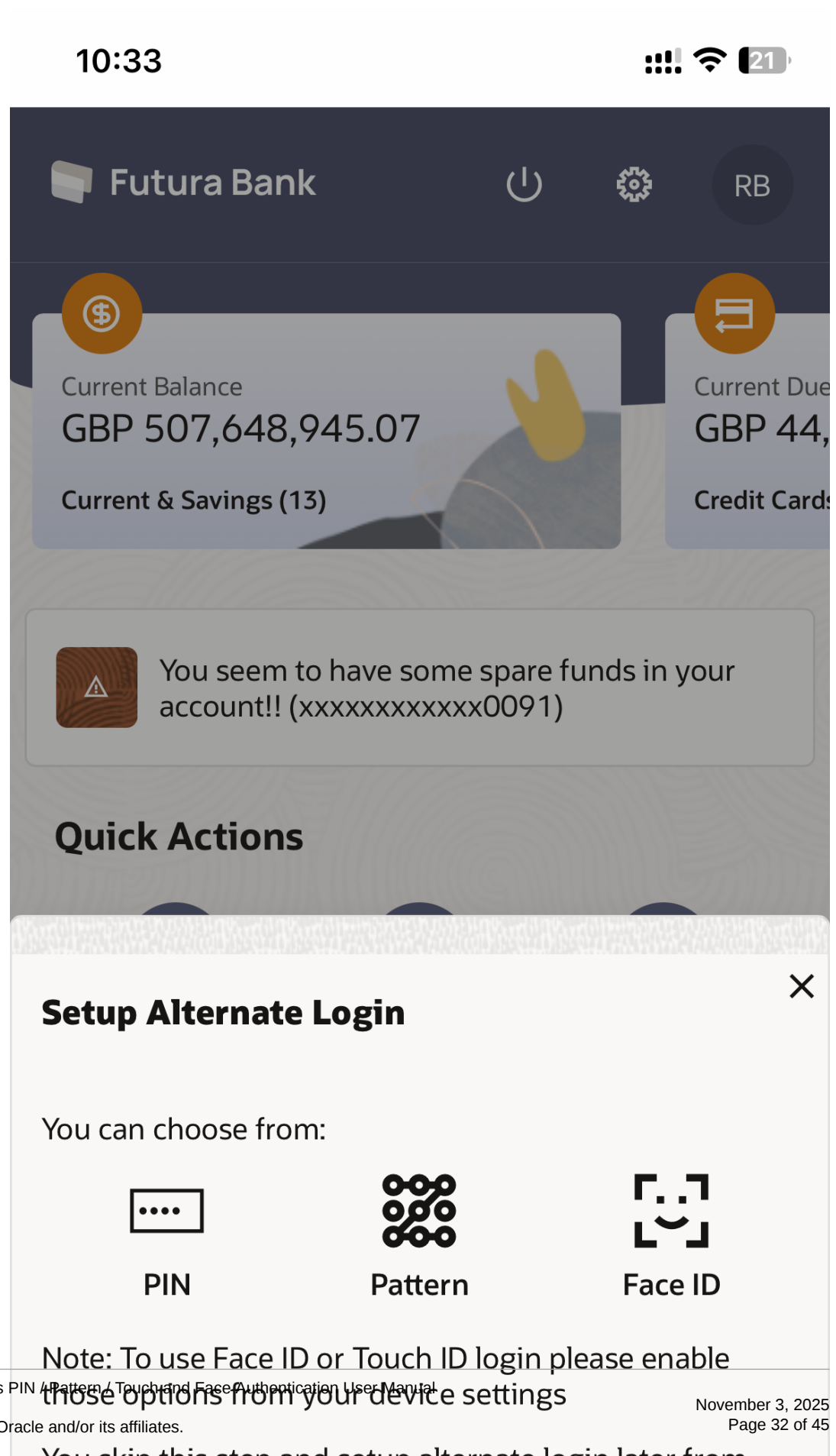
**Register**

[Copyright Statement](#)

2. In the **Username** field, enter the user ID.
3. In the **Password** field, enter the password.
4. Click **Login**.

The dashboard with **Select Alternate Login Method** popup screen appears.

Figure 1-17 Select Alternate Login Method screen- Face ID

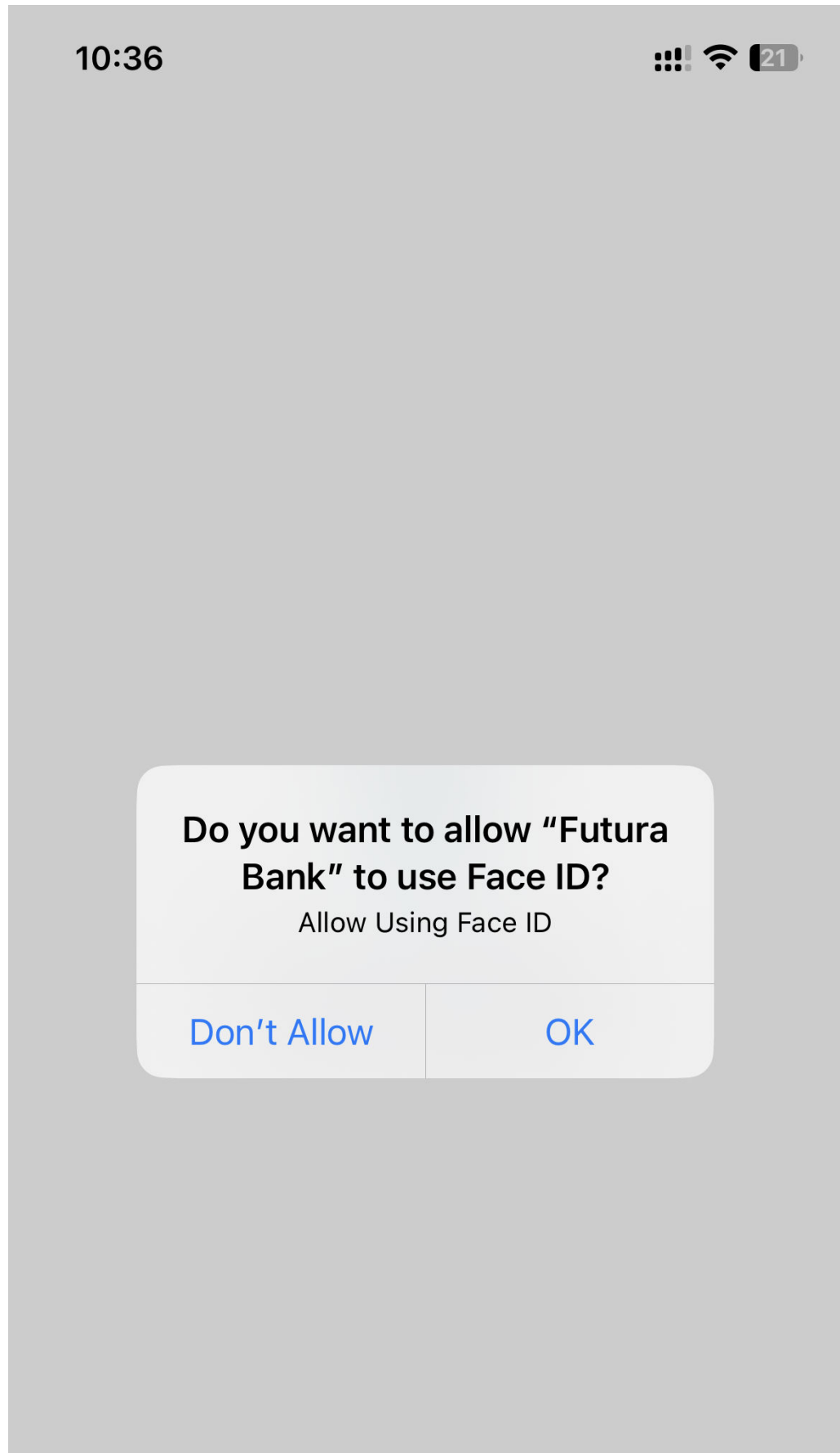




**Note**

- a. For registering **Alternate Login Method** on the User's device will automatically cancel the previous active registrations if any on other devices. Application verify user with unique identifier linked to device.
- b. User can click **Setup Later** and skipped and set later by navigating from the **Profile** → **Settings**. Refer **Manage Face ID** section for more information.

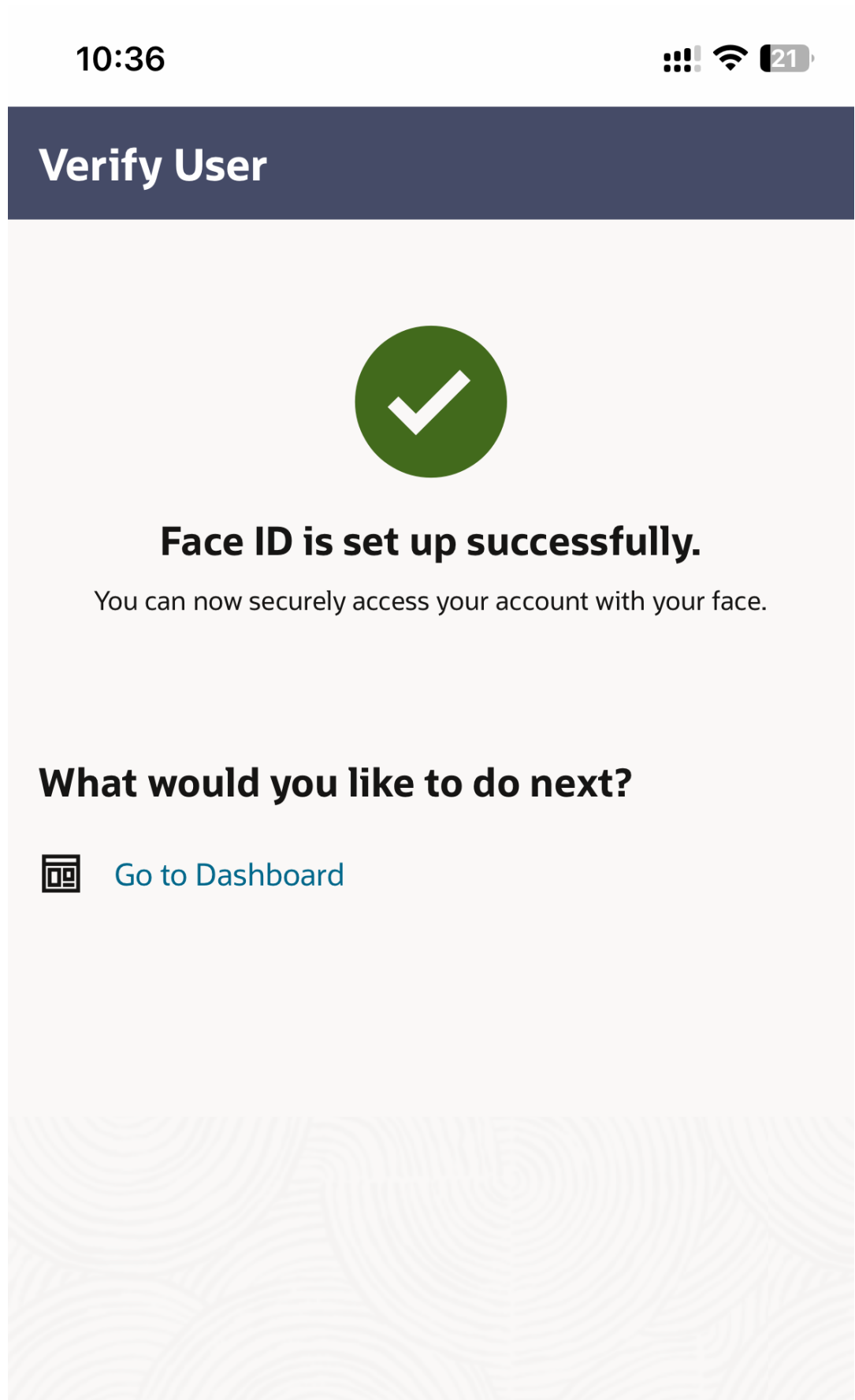
Figure 1-18 Face ID Authentication



5. Click **OK**.

The **Set Face ID** confirmation screen is displayed.

Figure 1-19 Success Message screen

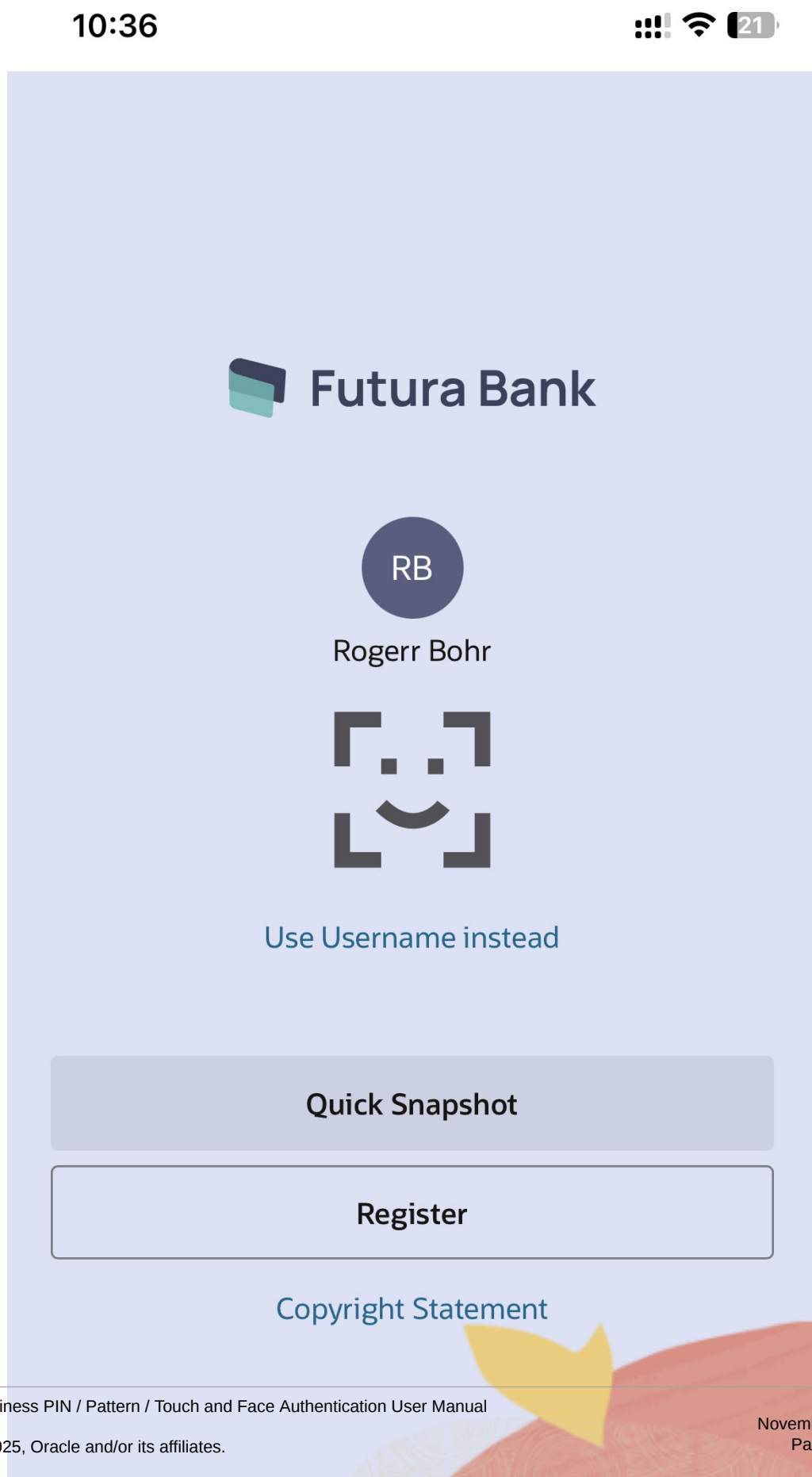


6. Once the **Face ID** recognition is successfully set as an alternate login, you will get an option to **Login with Face ID** on the login page.

## 1.3.2 Login using Face ID

This feature allows a user to login to Futura Bank mobile application with Face ID instead of entering their user ID and password after setting the Face ID as alternate login.

Figure 1-20 Login Using Face ID



**Note**

Click on the link **Use Username Instead** to log into application with user ID and password.

## 1.4 Touch ID Based Authentication

This option allows the user to login to the Futura Bank application using Touch ID recognition. The user also has the option of changing their alternate login from Touch ID to any other method.

**Features Supported In the Application:**

- [Set Touch ID](#)
- [Login using Touch ID](#)
- [Touch ID Recognition \(First Time Login\)](#)
- [Login using Touch ID](#)




### 1.4.1 Touch ID Recognition (First Time Login)


The user can define a fingerprint (touch ID) for login on the Futura Bank mobile application by entering the user ID and password.


**To set Touch ID for login transaction:**

1. Launch the **Futura Bank** application.  
The **Futura Bank** login page appears.

Figure 1-21 Futura Bank login

10:32   

 **Futura Bank**



[Forgot Password / Username](#)

**Login**

**Quick Snapshot**

**Register**

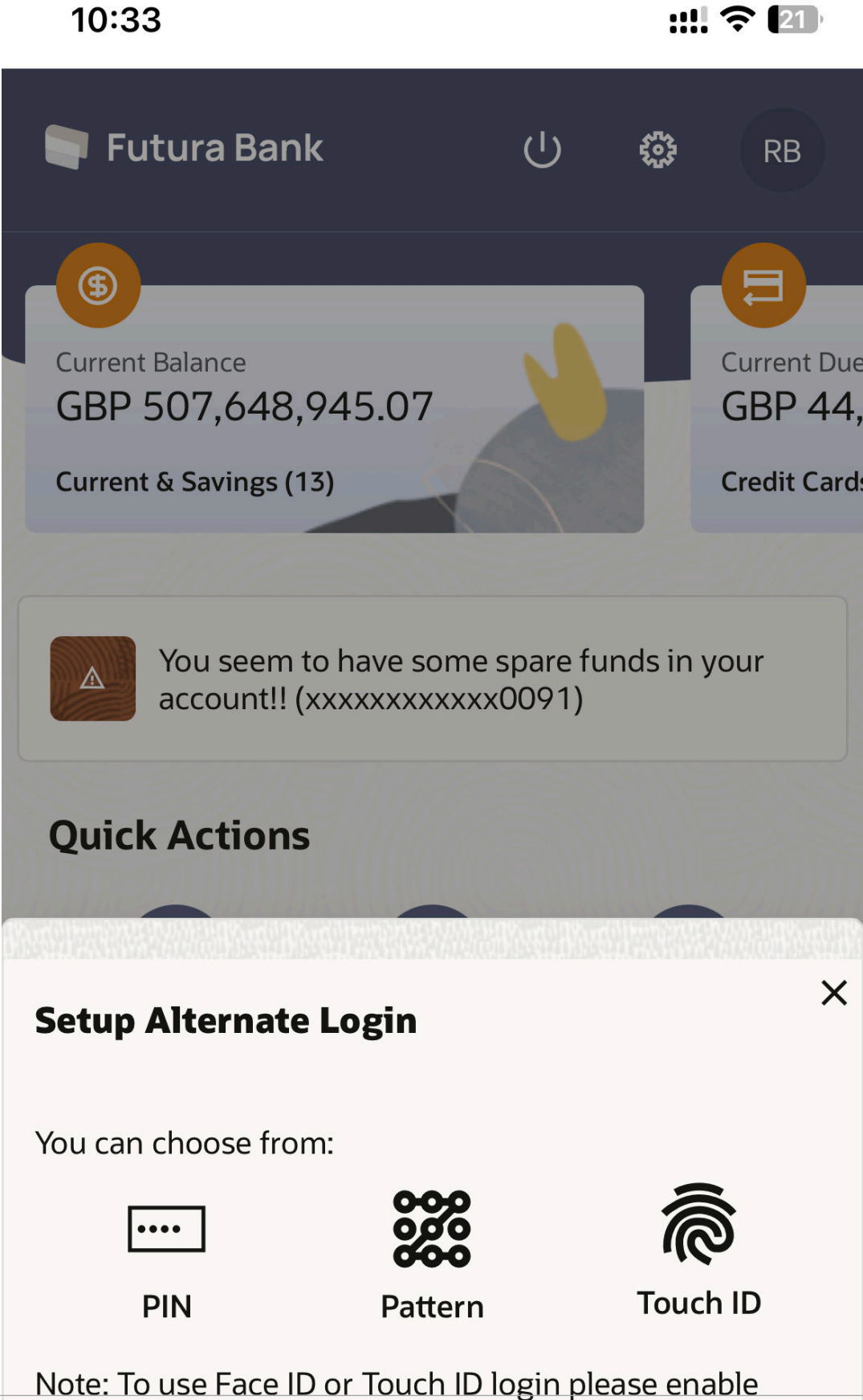
[Copyright Statement](#)



2. In the **Username** field, enter the user ID.
3. In the **Password** field, enter the password.
4. Click **Login**.

The dashboard with Select **Alternate Login Method** popup screen appears

Figure 1-22 Select Alternate Login Method screen- Touch ID



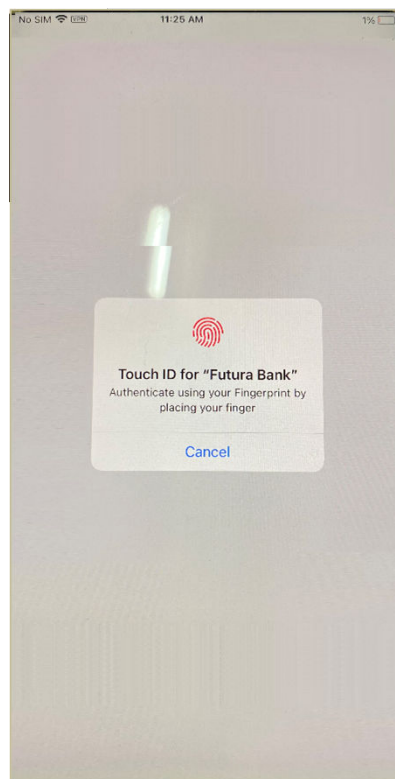
**Note**

- a. For registering **Alternate Login Method** on the User's device will automatically cancel the previous active registrations if any on other devices. Application verify user with unique identifier linked to device.
- b. User can click **Setup Later** and skipped and set later by navigating from the **Profile** → **Settings**. Refer **Manage Touch ID** section for more information.

5. Select the **Touch ID** based authentication method.

Once the fingerprint is authenticated, a message confirming the fingerprint recognition is displayed.

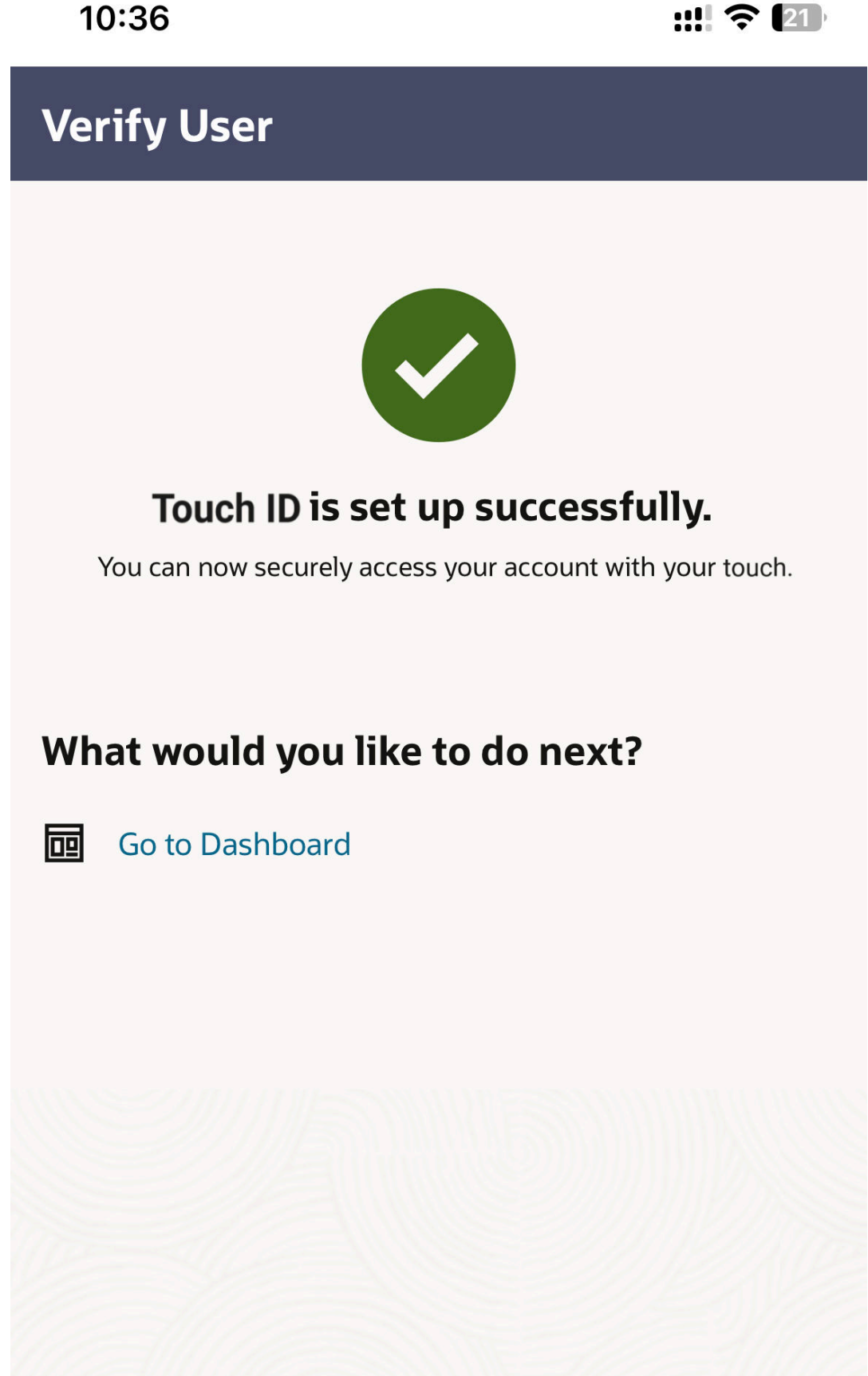
**Figure 1-23 Touch ID Authentication**



6. Click **OK**.

The **Set Touch ID** confirmation screen is displayed.

Figure 1-24 Success Message screen

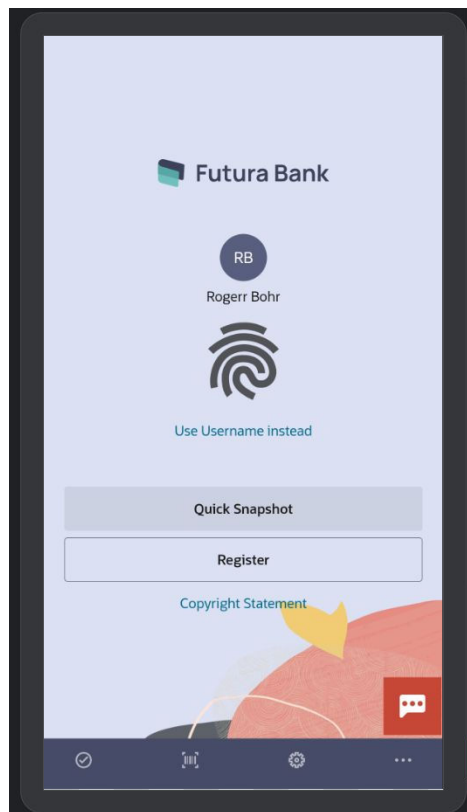


7. Once the **Touch ID** as an alternate login is successfully set, you will have an option to **Login with Fingerprint** on the login page.

## 1.4.2 Login using Touch ID

This feature allows a user to login to Futura Bank mobile application with Touch ID instead of entering their user ID and password after setting the Touch ID as alternate login.

**Figure 1-25 Login Using Touch ID**



### **Note**

Click on the link **Use Username Instead** to log into application with user ID and password.

# 2

## Using Alternate Login Method

1. Launch the **Futura Bank** application.
2. The system prompts you to enter a PIN or draw a Pattern or Login with Touch ID/ Fingerprint or Face ID based on the alternate login method you have selected.

Figure 2-1 Login Method screen- Pattern

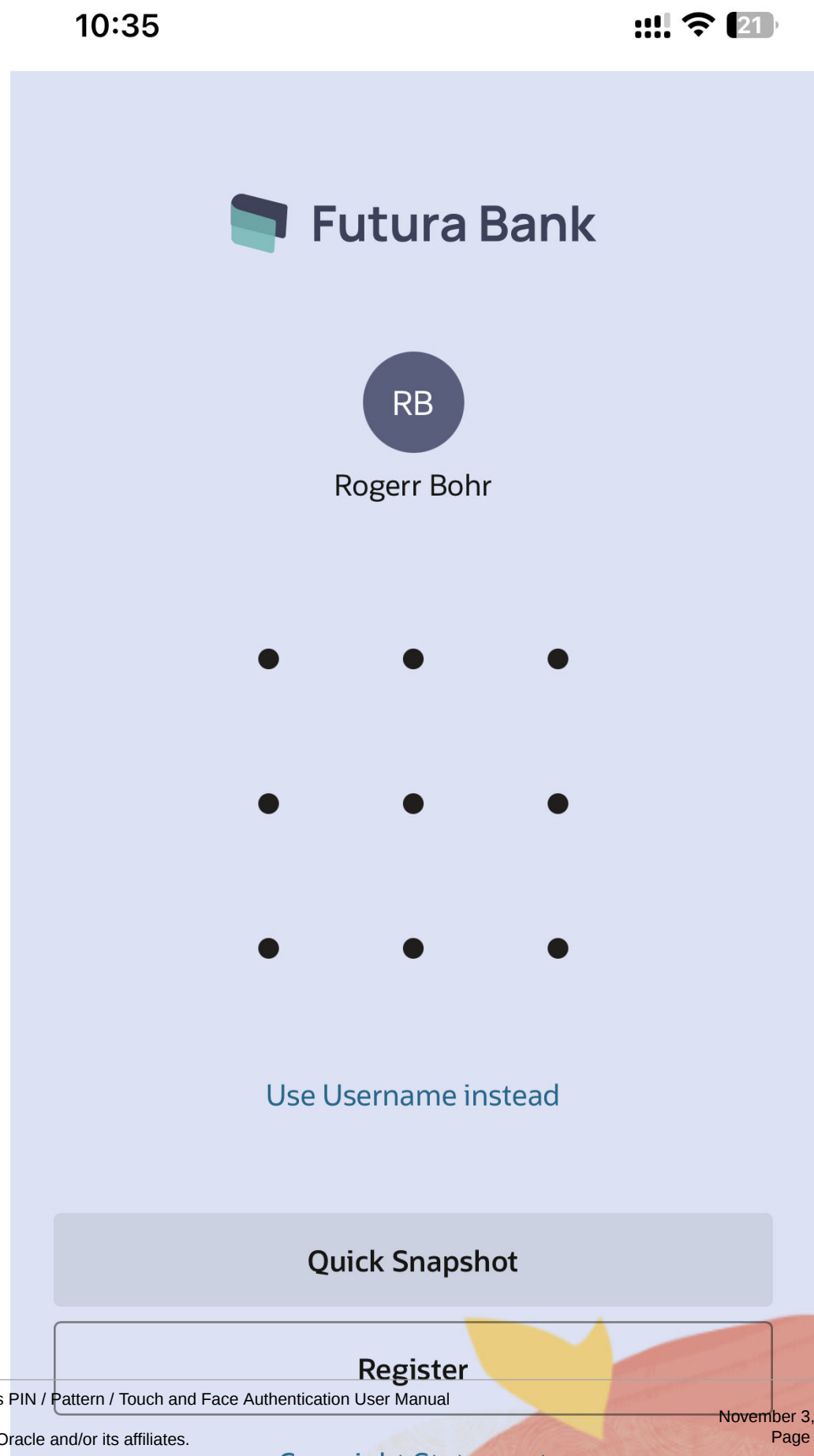


Figure 2-2 Login Method screen- PIN

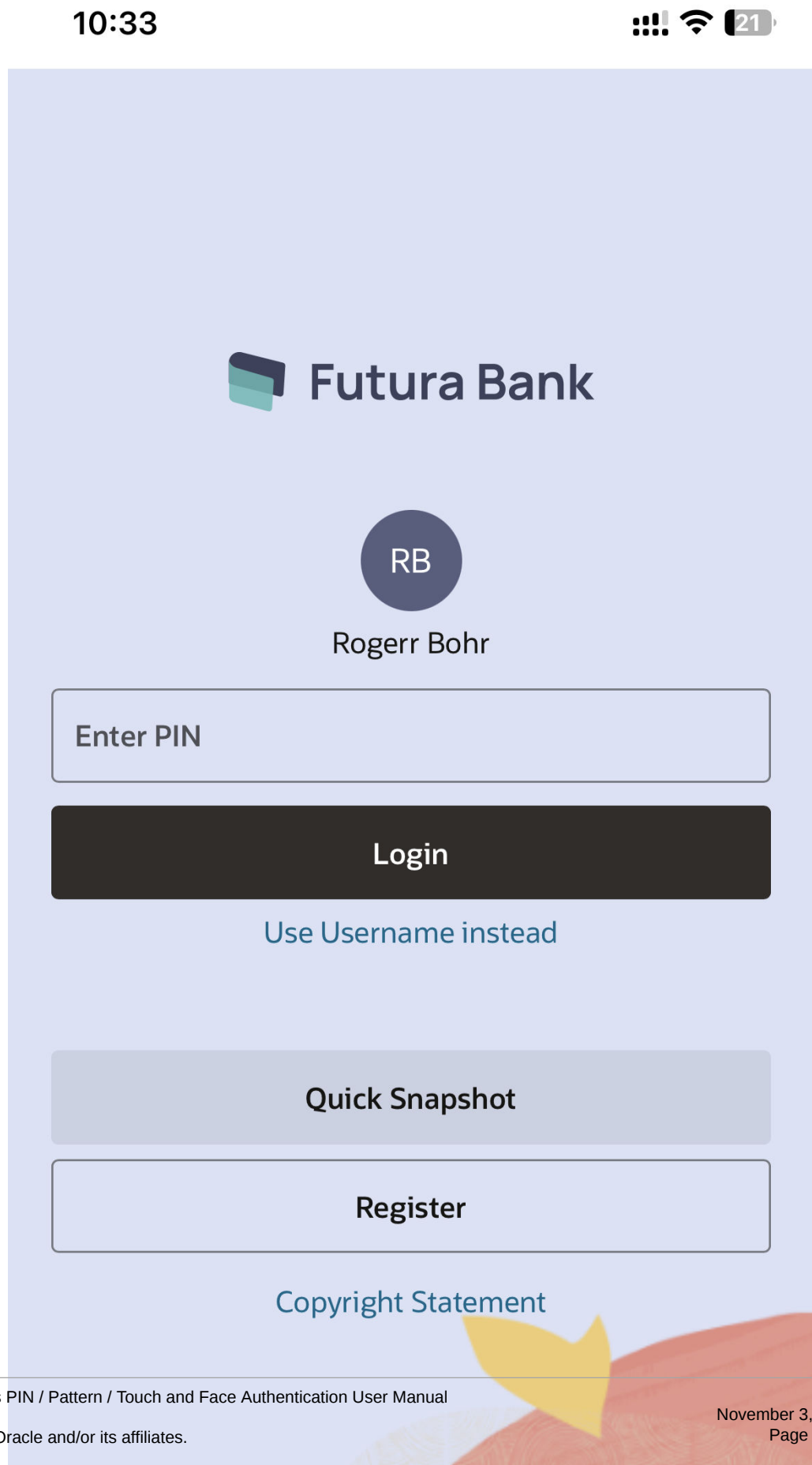
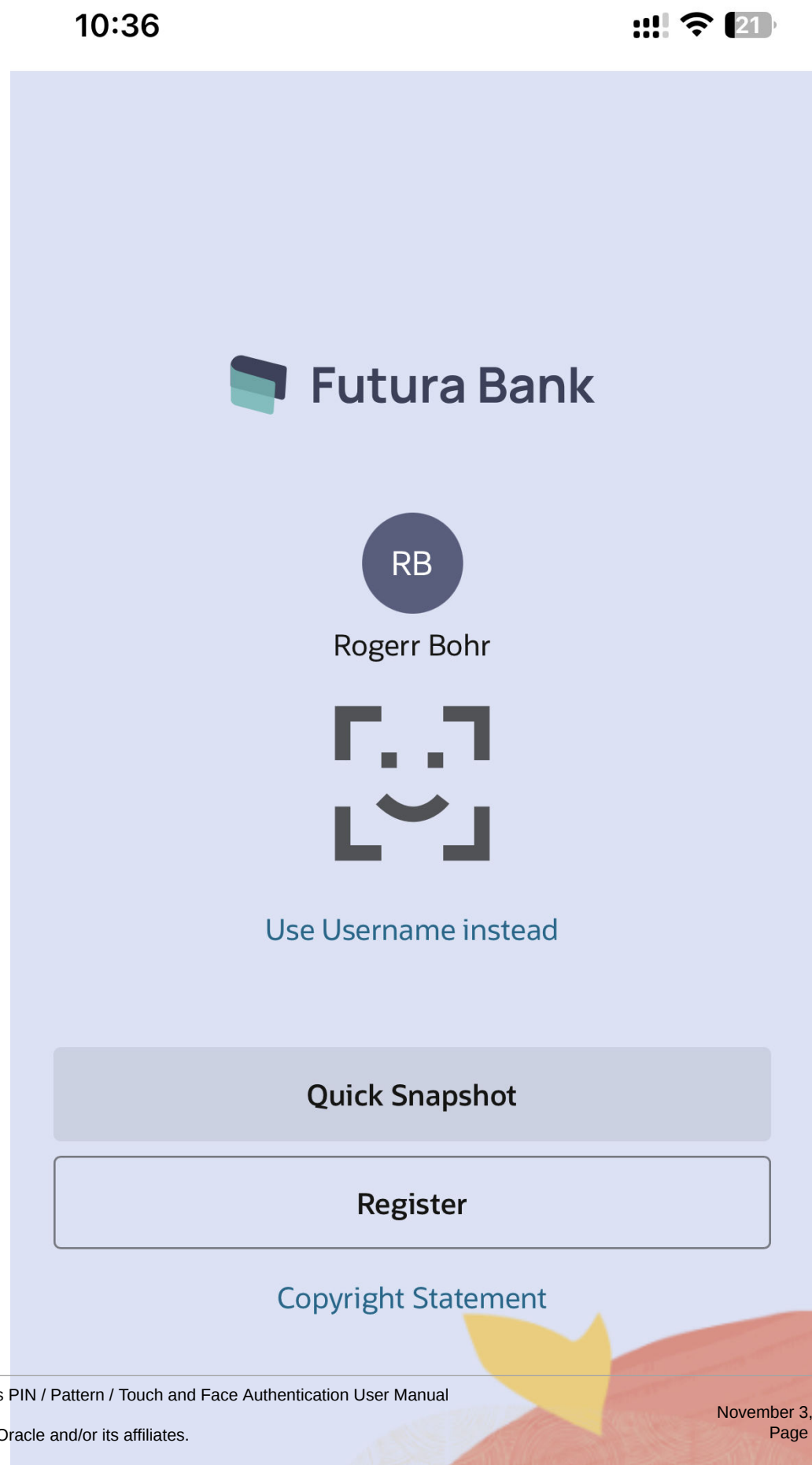
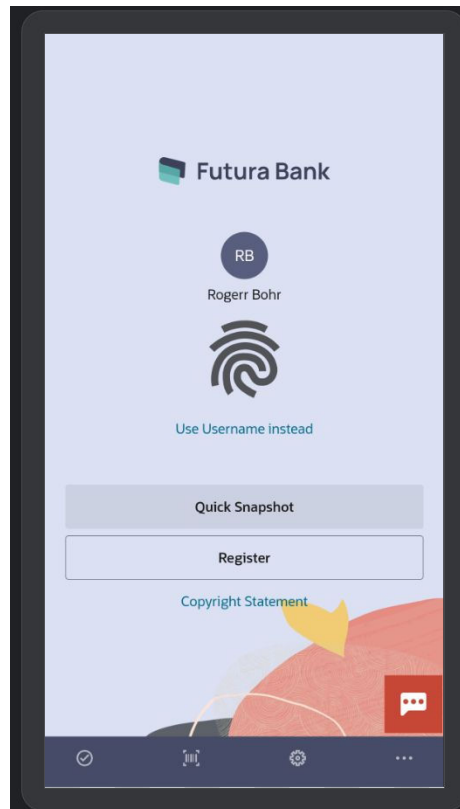




Figure 2-3 Face ID Login screen



**Figure 2-4 Touch ID Login screen**

3. If **PIN** is set as the authentication method, enter the **PIN** defined for login
4. If **Pattern** is set as the authentication method, draw the **Pattern** defined for login.
5. If **Face ID** is set as the authentication method, click **Login with Face ID**.
6. If **Touch ID** is set as the authentication method, click **Login with Fingerprint**.
7. On successful authentication, you get logged in to the **Futura Bank** application.

# 3

## FAQ

**1. What are the alternate login methods used in Mobile?**

PIN, Pattern, Touch ID and Face ID can be used as alternate login method for logging into the Futura Bank mobile application.

**2. How to modify the PIN or Pattern?**

Login to **Futura Bank** mobile application, then click **Profile Photo** → **Settings**, click **Alternate Login** and Select the option **PIN/Pattern**.

**3. If user re-installs the mobile application on a new phone, is it required to register the alternate login again?**

Yes, a user has to register the alternate login again on the new device.

**4. Can a user have two alternate login methods for authentication?**

No, a user can only set one type of authentication method, that is, PIN / Pattern / Touch ID / Face ID.

**5. What if the user has forgotten the defined PIN or Pattern?**

To reset the PIN/Pattern, login to **Futura Bank** mobile application, then click **Profile Photo** → Click on **Settings**, click **Alternate Login** and **Select PIN/Pattern**.

# Index

## F

---

Face ID Based Authentication, [29](#)  
Face ID Based- Set Face Recognition (First Time Login Flow), [29](#)

## L

---

Login using Face ID, [37](#)  
Login using pattern, [13](#)  
Login using PIN, [27](#)  
Login using Touch ID, [45](#)

## M

---

Manage Pattern, [11](#)  
Manage PIN, [25](#)

## P

---

Pattern Based Authentication, [1](#)  
PIN based Authentication, [15](#)

## S

---

Set Pattern (First Time Login Flow), [1](#)  
Set PIN (First Time Login Flow), [15](#)

## T

---

Touch ID Based Authentication, [39](#)  
Touch ID Recognition (First Time Login), [39](#)

## U

---

Using Alternate Login Method, [1](#)