



Ref: IPPB/OPS/PQ/SOP/ 2023-24/013

Date: 27.03.2024

SOP- Implementation of Two factor authentication in CBS - Finacle

Document Name	SOP – Implementation of two factor authentication in CBS-Finacle
Processing Unit	Branch/Banking outlets and CPC
Document Owner	Operations Dept.
Initial Document No. & Date	IPPB/OPS/PQ/SOP/2023-24/013 and 27/03/2024
Present Document No., Date & Version	IPPB/OPS/PQ/SOP/2023-24/013 ; 27/03/2024 ; V1.0
Security Classification	Internal and confidential
Criticality	Low (To be reviewed once a year or on need basis)

Approval Matrix

Sr No	Version	Description	Name	Designation	Role	Date	Signature
1	V1.0	Initial Version	BGP Diwaker	Sr Manager	Author	02/03/2024	Sd/-
			Kunal Mathur	Manager	Reviewer	04/03/2024	Sd/-
			Suhasini P	Manager	Reviewer	02/03/2024	Sd/-
			Ankur K	Sr Manager	Reviewer	04/03/2024	Sd/-
			Tarun P	Sr Manager	Reviewer	05/03/2024	Sd/-
			Vijyant M	DGM North Zone	Reviewer	20/03/2024	Sd/-
			Vijayan Kesavan	DGM Operations	Reviewer	20/03/2024	Sd/-
			Lavanya K Arumugam	GM Operations	Approver	21/03/2024	Sd/-

Contents

1.0	Introduction	3
2.0	Important Terms and Abbreviations.....	3
3.0	Process Flow.....	3
3.1	First time registration of Mobile number	3
3.2	2FA using OTP post CBS login using COTP menu	4
3.3	Changing the registered Mobile number using MOTP menu in CBS	5
3.3.1	Flow to handle request for Mobile number change	5
3.3.2	Steps involved in CBS for changing mobile number	6
3.3.3	Maker checker matrix for processing mobile number change requests	7
4.0	Approval matrix.....	8
4.1	Approval matrix for Mobile number change request	8
4.2	Approval matrix for exceptional bypassing of 2FA	8
5.0	Exception Management.....	9
5.1	Error Handling.....	9
5.2	Handling scenarios where the mobile number to be changed is already existing against any other user record	10
5.3	Bypassing 2FA in rare circumstances for a specific user/group of users	11
5.4	Miscellaneous exception handling.....	12
6.0	Escalation matrix.....	12
7.0	Frequently Asked Questions	12

1.0 Introduction

The goal of the document is to provide details about the implementation of Two factor authentication in CBS -Finacle. Steps involved like one-time registration, authentication using OTP and subsequent change management is included.

Two factor authentication or “2FA” is an established security control in Banking applications that adds a layer of enhanced control and prevents unauthorised access to application thereby reducing risks involved. Implementation of same in CBS-Finacle will strengthen information security and will be applicable to Bank users as well as those end users/other officials that are permitted access to a small set of specific menus in CBS.

2.0 Important Terms and Abbreviations






- Two factor Authentication (2FA) – A security protocol which employs two separate forms of identification of the user attempting to access an application/system.
- OTP - One-time password is a method of identification of a user of an application or a system and is generally used as an additional layer over and above the primary identification method.
- ROTP - A CBS menu in Finacle that will allow a user to register his/her mobile number on which he/she intends to receive OTP for login authentication
- COTP - A CBS menu in Finacle that shall be used to trigger OTP every time a user logs into Finacle.
- MOTP - A CBS menu that shall be used by circle CBS UAR SPOCs/CBS Admin team to change mobile number of a CBS user.
- UAR - User Access review. It mainly is done for CBS and every Circle and dept has 2 officials that are to act as CBS UAR SPOCs who will assist CBS Admin team in collating various User access review related data periodically for conducting User Access review of CBS. These SPOCs will also be assigned certain roles with appropriate work class to enables them to undertake certain activities like password resent etc.

3.0 Process Flow

3.1 First time registration of Mobile number

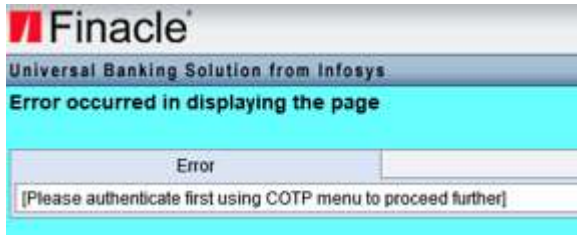
- As per the current practice, a user must log into Finacle using his/her current credentials (user ID and Password). There is no change in the same due to implementation of 2FA.
- The user must register his/her mobile number using ROTP menu to proceed further. Steps involved are as below,

Invoke ROTP menu in CBS	
-------------------------	--

<p>1.Account number field to be left Blank 2.Provide CBS user id in Employee ID field and Mobile number correctly</p>	
<p>3.Click on Validate Mobile Number button to trigger OTP. 4. Re-Send OTP button can be used if OTP not received earlier</p>	
<p>5. Enter the received OTP in “OTP Number” field</p>	
<p>6. If OTP is captured correctly, success message will be displayed. 7.Click on “OK” button in the pop-up message</p>	
<p>8. Click on “Submit” button to complete the registration of the mobile number using ROTP menu. Success message will be displayed.</p>	

3.2 2FA using OTP post CBS login using COTP menu

- If a user has already completed first time registration of his/her mobile number using ROTP menu as per sec 3.1, system would throw an error if user tried to invoke any menu post login. Error screen depicted below



- Above error means that post every login, user must invoke COTP menu, trigger the OTP and validate the same. Steps involved in COTP menu are as below,

<p>1. Invoke the COTP menu in CBS.</p>	
<p>2. Mobile number already registered will be displayed, Click on Validate Mobile number button. Re-send option can be used if OTP is not received.</p>	
<p>3. Capture the OTP received correctly and click on Validate OTP button.</p>	
<p>4. If in order, success message will be displayed. Click OK and then on Submit button to complete the authentication.</p>	
<p>5. Successful authentication message would be displayed. Now user can invoke any menu in CBS as per their access rights and continue.</p>	

3.3 Changing the registered Mobile number using MOTP menu in CBS

3.3.1 Flow to handle request for Mobile number change

- It may happen that a CBS user has changed his/her mobile number. In such a scenario, the new number must be registered in CBS to start receiving the 2FA OTP on the new

mobile number. To change the mobile number, a request in below format shall be shared in below format,

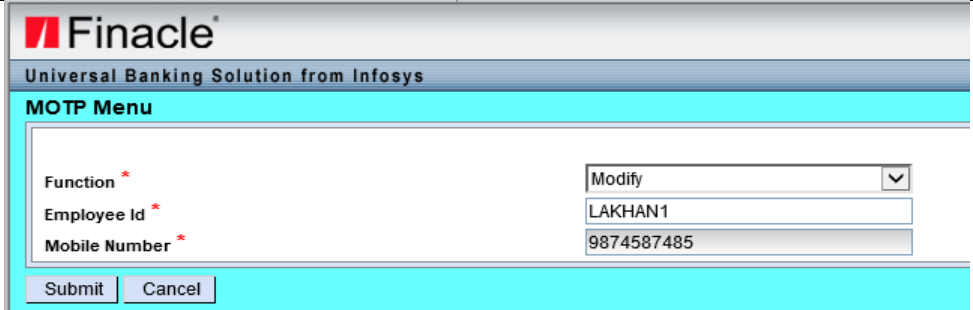
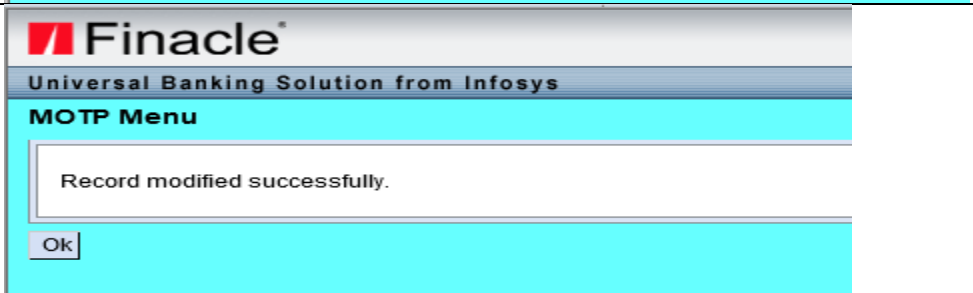
Date of request	User type	CBS user ID	Name of user	New mobile number	New Mobile number to be changed in AMS? (Yes/No)	SOL ID
-----------------	-----------	-------------	--------------	-------------------	--	--------

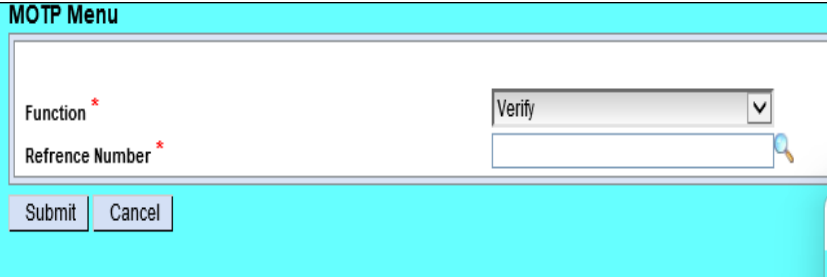
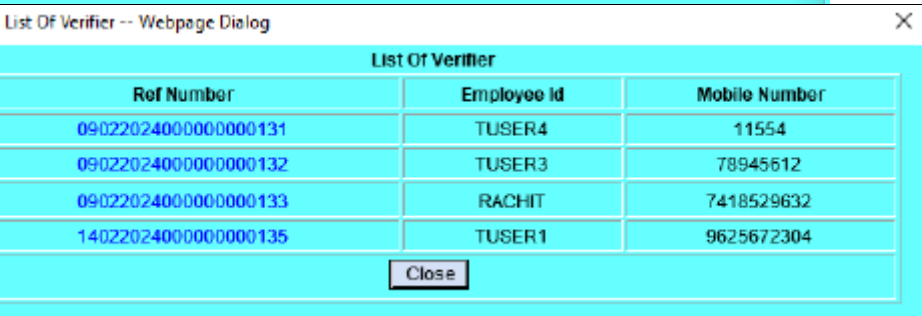
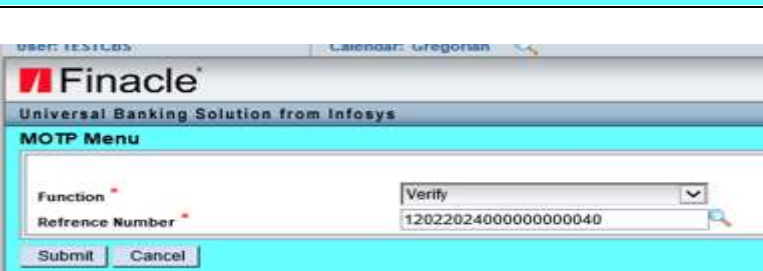
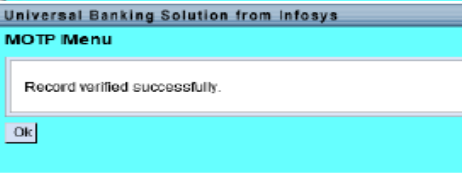
User Type, in above request format shall be filled up as one of the below values,

- BC End user – Any DoP staff with CBS access
 - Nodal PAO user – Any staff in Postal account office having access of CBS for recon purposes
 - Bank user – Any IPPB staff
 - Vendor staff – Any staff belonging to vendors working with Bank (like contact centre, IT support vendors, Support staffs at CPC etc.)
- Care shall be taken to quote correct mobile number, CBS user type and CBS user ID. If the new mobile number is also to be changed in AMS, it shall be mentioned as Yes, else as No. This flag won't be required for users other than BC End users.
 - Since 2FA is based on OTP validation, Mobile number change becomes very important and any such request must be duly forwarded by appropriate officials in DoP hierarchy (Like Sub division office/Division office or likes) for a BC end user.
 - For other user types, kindly refer to the Approval matrix for the same.
 - Requests can come through email or through hard copy. If hard copy, the same must be duly signed and duly forwarded.

3.3.2 Steps involved in CBS for changing mobile number

- MOTP menu shall be used for the same. This menu shall be accessible to only few users and maker-checker norms must be followed while using this menu.
- Steps involved in MOTP menu to change the registered mobile number for receiving 2FA OTP are as below,

<p>1. Maker user shall invoke the MOTP menu in CBS and use Function Modify. Capture the CBS user ID in Employee ID field and mention the new mobile number for registration. Click on Submit button to proceed.</p>	
<p>2. If the mobile number entered is not already mapped to some other existing user and is as per validation norms (like no special characters, 10 digits etc.), the new mobile number will get registered successfully.</p>	

<p>3. The checker user must verify the request for change in mobile number using verify function in same menu, MOTP.</p>	
<p>4. Click on the searcher in Reference number field to display all pending requests. Click displayed Ref Number to select a record.</p>	
<p>5. Click on Submit button to verify selected record.</p>	
<p>6. If in order, the record can be verified. Once verified, success message will be displayed appropriately.</p>	

3.3.3 Maker checker matrix for processing mobile number change requests

- Request for mobile number change for BC users shall be duly forwarded by branch/banking outlet official after having received the same properly approved by respective DoP hierarchy, as mentioned in the approval matrix.
- Once the request is received, it shall be cross checked for genuineness and recommended to CBS UAR SPOC in the circle for changing the mobile number using MOTP menu. Each Circle has 2 CBS UAR SPOC who shall be responsible for such changes as maker and checker users.
- For all other users, maker-checker matrix and approving authorities shall be as per the below table and as per the approval matrix.
- Maker-checker matrix is as below,

CBS user Type	Maker	Checker
BC users	CBS UAR SPOC at the respective Circle	CBS UAR SPOC at the respective Circle
Nodal PAO user	CBS Admin Maker user at CPC	CBS Admin checker user at CPC
Vendor staff at Corporate office	CBS Admin Maker user at CPC	CBS Admin checker user at CPC

CBA UAR SPOCs of Depts. or any other user not categorised specifically.	CBS Admin Maker user at CPC	CBS Admin checker user at CPC
Bank users other than CBS UAR SPOCs	CBS Admin Maker user at CPC	CBS Admin checker user at CPC

- It is to be noted that maker and checker users must be different. A user whose user id is being modified should **NOT** modify details for her/his own user ID.
- TAT for such requests for BC users should ideally be on same day and T+1 working day on exceptional basis. Requests received at CBS Admin team should get processed on T+1 working day basis. This is only an outer limit and ideally the requests should be processed immediately upon receipt as it involves user being unable to log into system to perform his/her daily task.

4.0 Approval matrix

4.1 Approval matrix for Mobile number change request

- As the mobile number change is sensitive from the perspective that the 2FA OTP would go to the number, any such change would be subjected to a prior recommendation or approval as per the matrix below,

CBS User Type	Approving Authority	Remarks
BC end users	Respective DoP Hierarchy	Division/Sub Division/HPM . Forwarding request in proper format as per sec 3.3.1 through official email is a must
Nodal PAO user	PAO Nodal office	State Nodal PAO user can send request to PAO Nodal office, Delhi that will recommend and send request to CPC Nodal office (IPPB). CPC team shall forward the request to CBS Admin team for fulfilment
Vendor staff users	Respective Section/vertical official heading the team to which vendor user is tagged.	Such requests shall be sent to respective CBS UAR SPOCs of the dept. that shall process the request
CBS UAR SPOC's and other users not categorised specifically	Circle UAR-SPOC users – Circle Head CBS UAR SPOC users at Corporate office- AGM or above in the Dept.	Request format in mail shall be duly forwarded by approving authority to CBS admin team in CPC at assist.operations@ippbonline.in
Bank users other than CBS UAR SPOCs	Bank users other than CBS UAR SPOCs can directly send mail to CBS admin team for mobile number change from their personal email id (xxxxx@ippbonline.in)	Mails to be sent to assist.operations@ippbonline.in

4.2 Approval matrix for exceptional bypassing of 2FA

In the rare scenario, if 2FA is to be bypassed for a specific user or group[#] of users, the same shall be duly approved as below,

CBS User Type	Recommending Authority	Approving Authority
BC End user	Branch Manager	Regional/Circle Head or above
Bank user in Branch/banking outlet	Regional Head* or above	Circle Head or above
Bank user at Regional office	Regional head or above	Circle Head or above
Bank user at Circle Office	Circle head or above	Zonal Head or above or AGM or above at Operations Dept.
Bank user at Zonal office	Zonal head	DGM or above at operations Dept.
Bank user at Corporate office	AGM or above of the Dept.	Head of the Dept.
Vendor users	AGM or above of the Dept.	Head of the Dept.



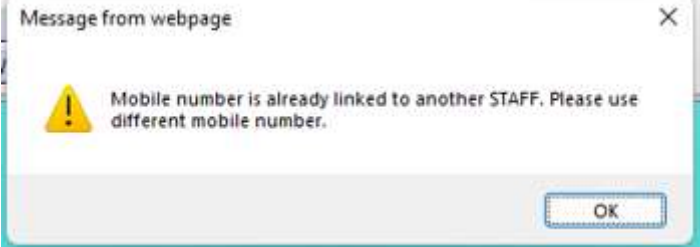
*In case of a circle that does not have Regions, Circle Head alone shall approve.

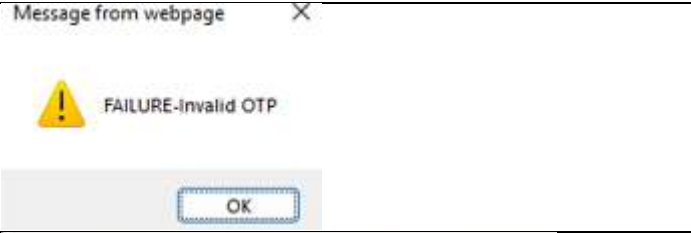


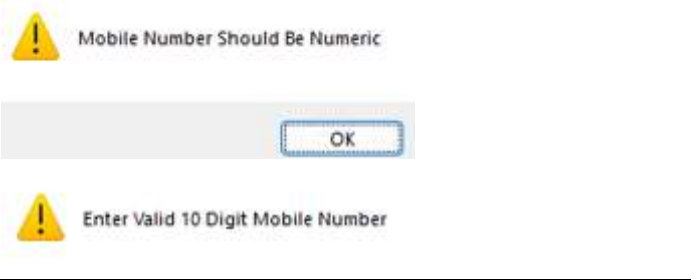

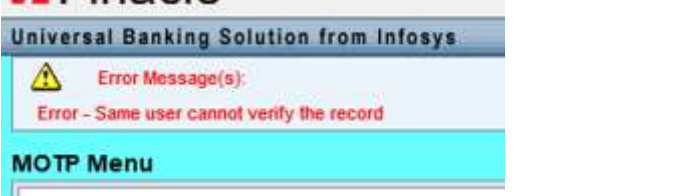
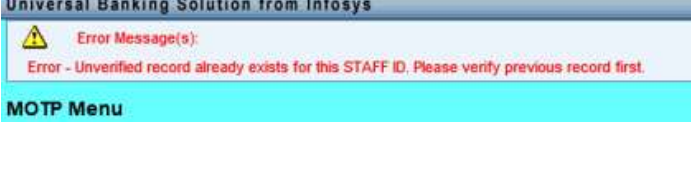
#In case of more than one such users, a list can be annexed along with recommendation/approvals. Such requests can be processed basis e-mail approval.

5.0 Exception Management

5.1 Error Handling

- During the process of registration of mobile number using ROTP menu, subsequent 2FA post log in using COTP menu and invocation of MOTP menu for mobile number change may result in few error scenarios. Such error scenarios are designed to manage exceptions and users must be aware what those exception errors mean and what should the next step be. List of such error screens and suggested steps to be taken are listed below for reference,

Error screens with scenario	What does it mean?	What to do?
	User tried to Invoking any menu in CBS without doing 2FA using COTP.	Use COTP menu to undertake 2FA and validate the OTP
	User tried to use COTP menu for 2FA OTP without doing first time registration using ROTP	Use ROTP menu to register mobile number first then use COTP to validate.
	User tried to register in ROTP using a mobile number that is already linked to any other existing user.	Recheck the mobile number. If correct, this needs to shared with CBS Admin team at assist.operations@ippbonline.in for exception handling as per sec 5.2

	<p>User entered incorrect or expired during OTP validation.</p>	<p>Enter correct OTP or use re send OTP option to get a new OTP.</p>
	<p>User trying to register in ROTP menu with User ID that already has been registered before.</p>	<p>Recheck the CBS user id and enter again.</p>
	<p>Using MOTP menu. Mobile number change was initiated even before registering through ROTP.</p>	<p>Only a registered user can change mobile number. Register first using ROTP.</p>
	<p>User entered incorrect mobile number format like less/more than 10 digit, special characters, alphabets etc.</p>	<p>Please provide valid 10 digit mobile number only.</p>
	<p>During mobile number change, a number already linked to an existing CBS user was provided for change in MOTP menu.</p>	<p>Since this number is already linked to an existing user, check the number again and provide correct number. Else approach CBS Admin team at assist.operations@ippbonline.in for exception handling as per sec 5.2</p>
	<p>Maker user in MOTP trying to verify the changes made by her/him.</p>	<p>Checker user must be a different user. Assign to appropriate checker user.</p>
	<p>Maker user in MOTP menu trying to modify a record that is already modified but remains unverified.</p>	<p>Request Checker user to cancel or verify first using MOTP menu.</p>

5.2 Handling scenarios where the mobile number to be changed is already existing against any other user record

- It may happen that a user has changed her/his mobile number and placed the request to modify the same through MOTP menu. The maker user tries to make changes with the mobile number received. But if such a number already is available in system marked against any other user, then update will fail.

- There may be a rare scenario where such a mobile number was provided to a CBS user by Mobile service provider (MSP) company because the said number was not being used by the person to whom it was allotted before and MSP's can then allot such numbers to new customers after certain fixed period of inactivity.
- In such rare cases where both the previous allottee and the current holder of the number happens to a CBS user, above scenario may materialise and system won't allow any changes ordinarily.
- For handling such cases, appropriate mail request shall be shared with CBS admin team at assist.operations@ippbonline.in detailing the scenario along with error screen shot and mobile number proposed to be considered for change.
- CBS Admin team shall obtain details of existing users linked to the said mobile number from IT SPOC and peruse the user activity. CBS Admin team shall check with Branch/banking outlet or concerned Bank user/office/Dept. regarding the fate of CBS user and whether it can be deleted/removed. If the user has not undertaken any CBS activity or not logged in for considerable time, or was reported in monthly UAR as a user to be disabled/temporary delete etc. those could be perused by Admin team before sending such mails to provide appropriate information.
- If positive repose is received, users shall be deleted and mobile number mapped against them would be removed with the help of IT SPOC team. Post completion of activity, the requesting team shall be intimated to proceed with ROTP menu to change the mobile number.
- This activity is an exception handling and might involve multiple requests being exchanged and may take time. However, CBS Admin team shall be the owner for resolving the issue at the earliest.
- A record of such requests received shall be diarised by CBS admin team for future reference in below format,

New CBS user ID attempting change	Proposed mobile number	Existing CBS User ID	Existing user status	Response remarks from concerned branch/banking outlet/office/Dept	Date of receipt of request	Date of resolution
-----------------------------------	------------------------	----------------------	----------------------	---	----------------------------	--------------------

5.3 Bypassing 2FA in rare circumstances for a specific user/group of users

Though 2FA is essential, there may be rare scenarios where a specific user or group of users may need to be exempted from the same due to localised issues like lack of mobile device to receive OTP, in case such users are not allowed to keep mobile devices with them during business hours. Such user/user groups make request to their competent approving authority, as per sec 4.2, and share the details/list of such users with CBS Admin team that will get the exemption required by taking up the matter with concerned IT SPOC and respond back to the requesting user. Such requests shall be sent to assist.operations@ippbonline.in in the following format.

Date of request	User type	CBS user ID	Name of user	Dept./vertical/section	Reason for request	Approving authority name	Approving authority designation
-----------------	-----------	-------------	--------------	------------------------	--------------------	--------------------------	---------------------------------

User Type, in above request format shall be filled up as one of the below values,

- BC End user – Any DoP staff with CBS access
- Nodal PAO user – Any staff in Postal account office having access of CBS for recon purposes

- Bank user – Any IPPB staff
- Vendor staff – Any staff belonging to vendors working with Bank (like contact centre, IT support vendors, Support staffs at CPC etc.)

5.4 Miscellaneous exception handling

- Wherever applicable, exception scenarios have been mentioned in the document to the extent possible. However, all such scenarios may not be possible to list as these are exceptions and can happen in newer ways. For such exception scenarios, the officials in the designation of AGM or above in the Operations Dept. at the Corporate office shall have the power to ratify or approve such exceptions. Request for such ratification/approval shall be addressed by field functionaries to CBS Admin team which shall obtain necessary approvals from competent authority and inform the same to field officials accordingly.
- In case of any difference of opinion about the interpretation of any specific clause, the opinion of the Process Quality team shall be obtained and the same shall take precedence.

6.0 Escalation matrix

Escalations if any can be addressed to CBS Admin team at assist.operations@ippbonline.in or officials in operations dept as listed below.

Escalation Level	Contact person	Contact Details
Level 1	CBS Admin Team	assist.operations@ippbonline.in
Level 2	Suhasini P	suhasini.p@ippbonlin.in
Level 3	Ankur.K/Naveen R	ankur.k@ippbonline.in naveen.r@ippbonline.in

7.0 Frequently Asked Questions

1. *What is Two Factor Authentication or 2FA and why is it required to be done. CBS was working fine even without it. Why make it cumbersome to log in?*

Two factor authentication provides an added layer of security controls and safeguards to Bank's system containing information of customers. This also helps to prevent unauthorised access to the system. 2FA is an incremental effort to strengthen existing controls during login into CBS and can be easily undertaken by validating the OTP received that gets triggered using COTP. The process is very simple and will take less than a minute.

2. *What are the various menus to be used?*

Various menus to be used are as below,

ROTP- First time registration of mobile number on which OTP is to be received

COTP- To trigger and validate OTP post log in into CBS every time

MOTP- To change mobile number in future

3. *I have changed my mobile number but system is throwing error while changing the same. What to do?*

Please re-check and enter the correct mobile number. If mobile number is correct , refer sec 5.2 and follow the exception handling process.

4. Is an approval required to change the mobile number?

Yes. Given the sensitivity of mobile number as 2FA OTP would be received on the same, approval would be required. Approving authority for various CBS user types are mentioned in Approval matrix sec 4.1. Please refer the same.

5. I am unable to log in because OTP is not being received due to network issues. What to do?

In rare cases, such requests can be considered for exception waiver if duly approved by competent authority. Please refer sec 5.4 for exception handling

6. I got a call asking for OTP received to log in to CBS from my office colleague. Can it be shared in exceptional/exigencies to process transactions?

2FA OTP is equivalent to password and must **NOT** be shared with anyone under any circumstances. If done, such instances would be violation of Bank's policy in this regard and can have serious consequences. As a prudent practice, never share your password or OTP with any one, not even your office colleagues.