Merchant QR Code Application

USER MANUAL

Version 1.0

© 2020 Bornfire Innovations Private Limited

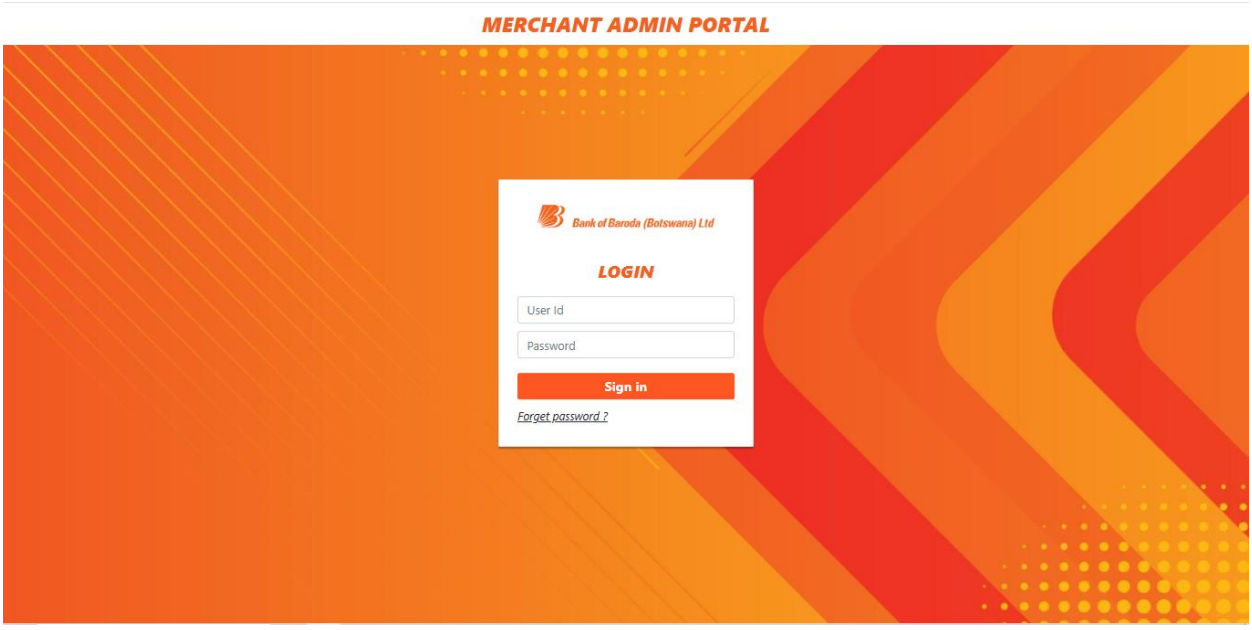
www.bornfire.in

Contents

1. Merchant Administrator 4
2. Merchant Dashboard 4
2.1. Merchant Master 4
2.2. Merchant Operations 25
2.2.1. Admin Operations 25
2.2.1.1. User Management 26
2.2.1.2. Device Management 27
2.2.1.3. Customer Transactions 28
2.2.1.4. Fees and Charges 30
2.2.1.5. Charge Backs 31
2.2.1.6. Alert and Notification 35
2.2.1.7. Service Request 37
2.2.2. Merchant QR 38
2.2.2.1. Static QR 39
2.2.2.2. Dynamic QR 40
2.2.3. Customer QR 41
2.2.4. Transaction Details 43
2.3. Reports 44
2.3.1. Transaction Report 44
2.3.2. Charge Back Report 45
2.4. Change Password 47
2.5. Two Factor Authentication 48
2.6. Forgot Password 50

Login Operation

Login Screen



Login Credentials

The following are the login validations.

- The user should have a Userid in the "User Profile" table.
- Valid password and it should be in force within the password life cycle.
- User record should be in active status.
- Login should be within the login low and high time.
- Should not be disabled.
- Should have a valid "Role Id" for accessing the menu options.
- User can access the menu / screen options according to "Role Id".
- User can perform operations according to the rights available for the "Permissions".
- Application keeps records of login attempts with 'Success' and 'Failure' status.

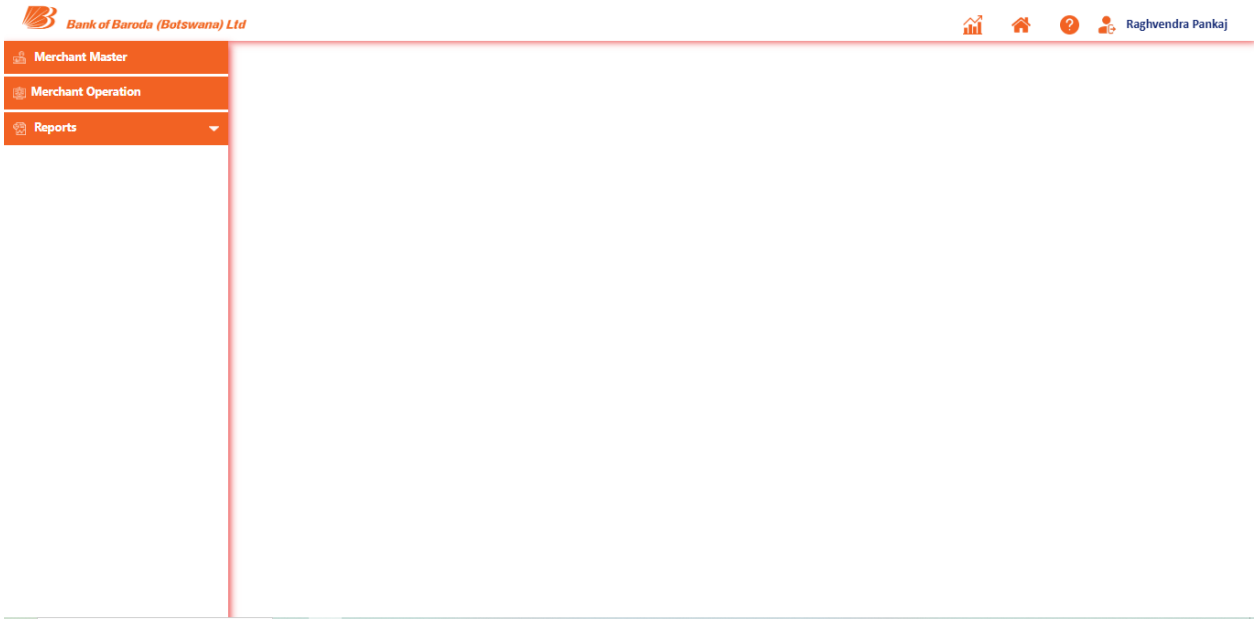
1. Merchant Administrator

Merchant Modules

- Merchant Master
- Merchant Operation

2. Merchant Dashboard

In the merchant dashboard, we display the total count of transactions and also represent them using a pie chart. Additionally, we provide the total count of devices and users, along with an option menu for logout and changing passwords.



2.1. Merchant Master

In the merchant master module of a banking system, merchants have the authority and functionality to manage various aspects related to their business operations.

In this module, merchants can create counter users, configure devices with unit-wise specifications, as well as verify and modify them.

Creation of Counter Users

Merchants can create accounts for counter users who are employees or representatives working at their physical locations, such as retail stores or service centers.

These counter users are typically responsible for conducting transactions, assisting customers, and managing day-to-day operations at the merchant's establishment.

Verification of Counter Users:

Merchants can verify the credentials and permissions of counter users to ensure that only authorized individuals have access to sensitive functionalities within the system.

Verification may involve confirming the identity of counter users through documentation or authentication processes to mitigate risks associated with unauthorized access or fraudulent activities.

Configuration of Devices with Unitwise Specifications

Merchants have the ability to configure devices such as POS terminals, card readers, or other hardware used for processing payments and managing transactions.

They can specify unit wise details for each device, including settings related to currency, language, transaction limits, and security protocols.

Modification of Counter Users and Devices:

Merchants have the flexibility to modify the details and settings of existing counter user accounts and devices as needed.

This includes updating user information, adjusting access permissions, or reconfiguring device settings to align with changes in business requirements or operational workflows.

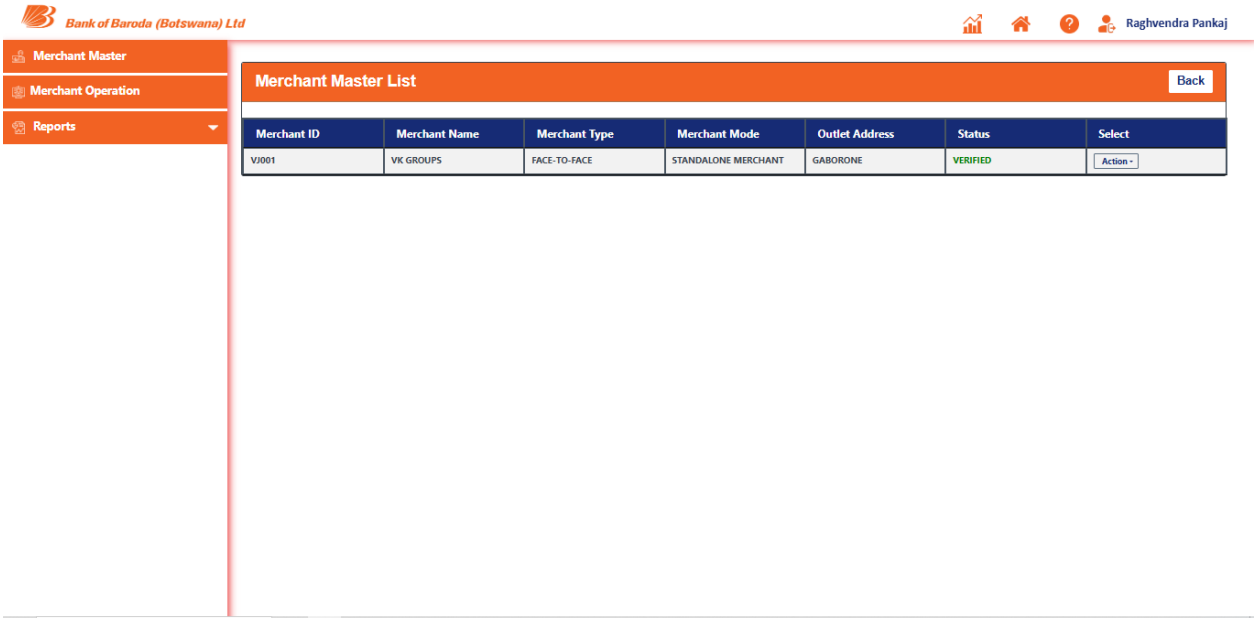
Verification and Modification of Merchant Details:

Additionally, within the merchant master module, merchants can verify and modify their own account details and business information.

This allows merchants to keep their profiles up to date with accurate contact information, business addresses, product or service offerings, and other relevant details.

Merchant Master-List

Displays a list of Merchant Master. The Screen will appear below,



Merchant Master –View

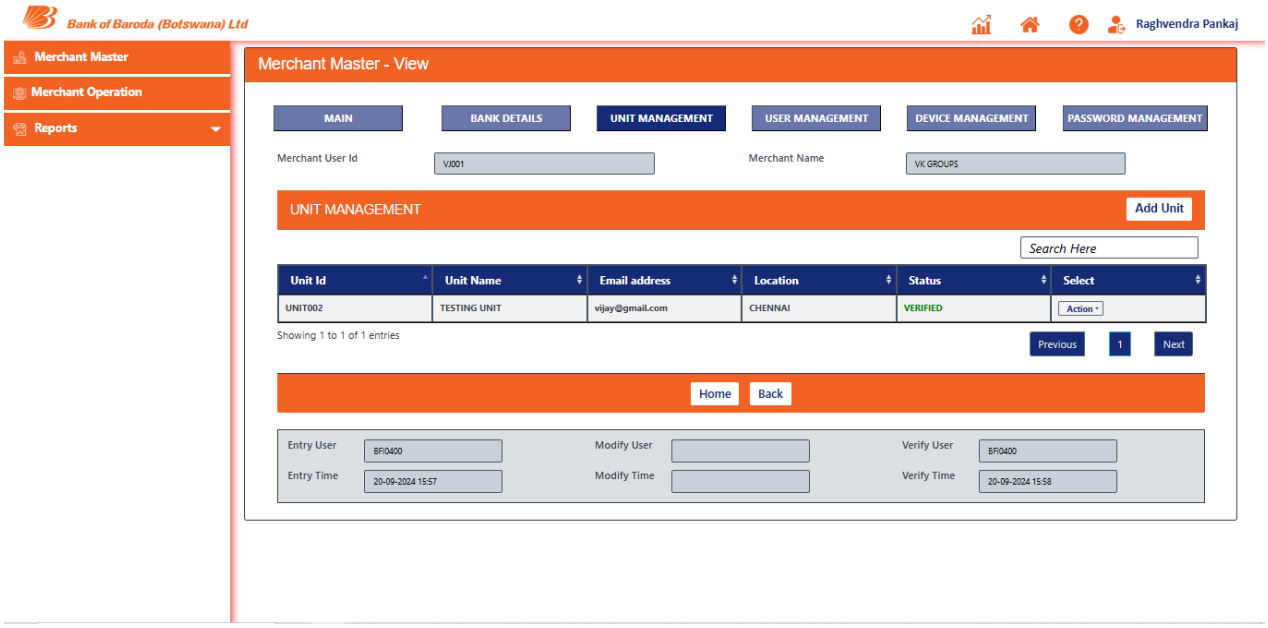
Displays the view of the selected record from Merchant details .The Screen will appear below,

Merchant Master –Bank Details

Displays the view of the selected record from Bank details. The Screen will appear below,

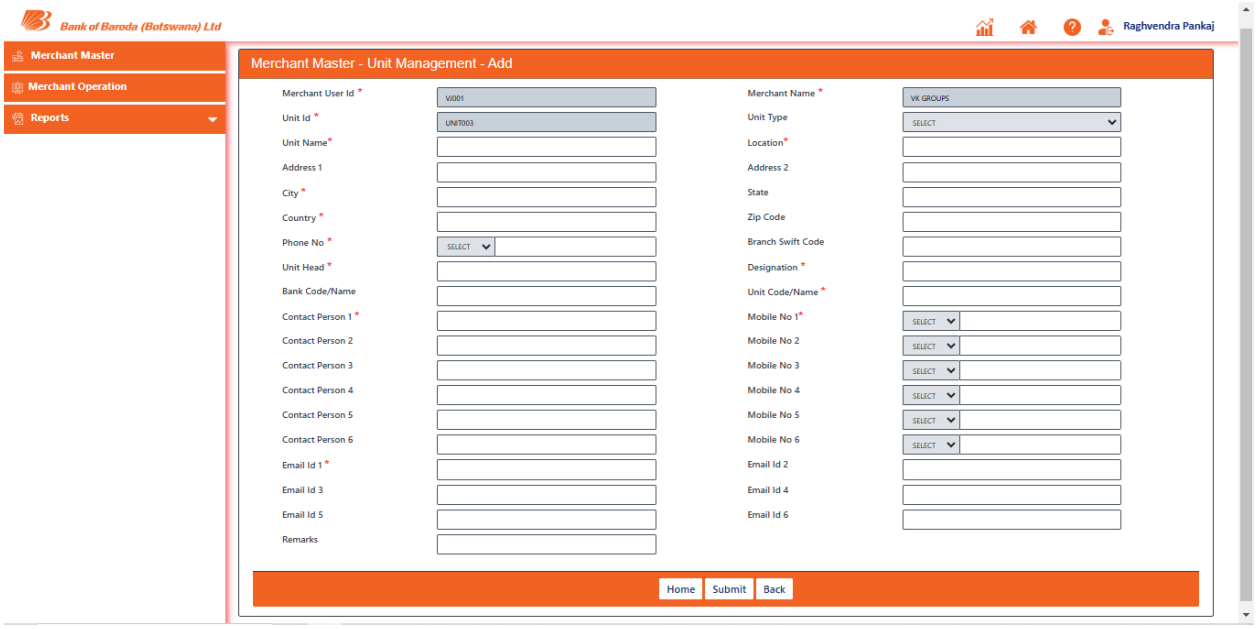
Merchant Master –Unit Management List

Displays a list of Unit management . The Screen will appear below,



Merchant Master –Add Unit Management

- Merchants can manage their users effectively in the user management section.
- Users can be added under the specific merchant currently logged in.
- Counter user details are collected for each user added.
- All mandatory fields must be filled out.
- After filling out the details, the information should be submitted.
- After submitting the user details, the verify status is set to unverified.
- The unverified status requires verification.

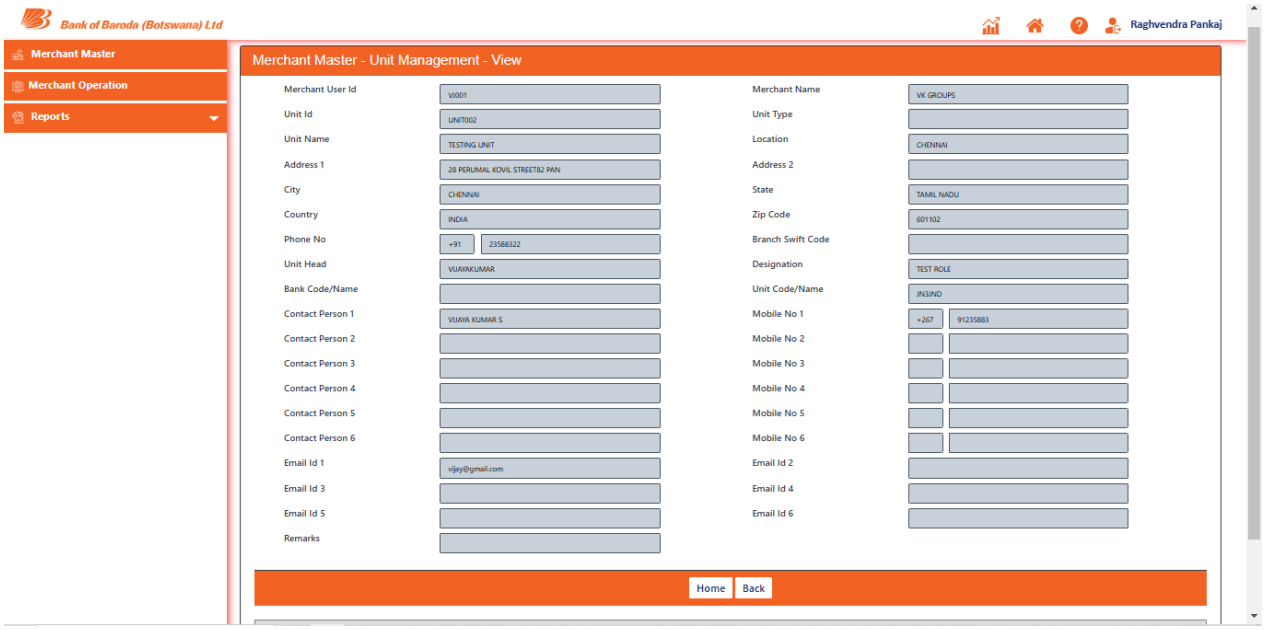


Unit Management		
Mandatory Field	**User Action**	**Description**
Unit Id	Displayed	Mandatory Free Text Alphanumeric
Unit Type	Displayed	Mandatory Free Text Alphanumeric
Unit Name	Displayed	Mandatory Free Text Alphanumeric
Location	Displayed	Mandatory Free Text Alphanumeric
City	Displayed	Mandatory Free Text Alphanumeric
Country	Displayed	Mandatory Free Text Alphanumeric
Phone Number	Displayed	Mandatory Free Text Alphanumeric
Branch Swift Code	Displayed	Mandatory Free Text Alphanumeric
Branch Head	Displayed	Mandatory Free Text Alphanumeric
Designation	Displayed	Mandatory Free Text Alphanumeric

Bank Code	Displayed	Mandatory Free Text Alphanumeric
Branch Name	Displayed	Mandatory Free Text Alphanumeric
Contact person 1	Displayed	Mandatory Free Text Alphanumeric
Mobile number 1	Displayed	Mandatory Free Text Alphanumeric
Email Id 1	Displayed	Mandatory Free Text Alphanumeric

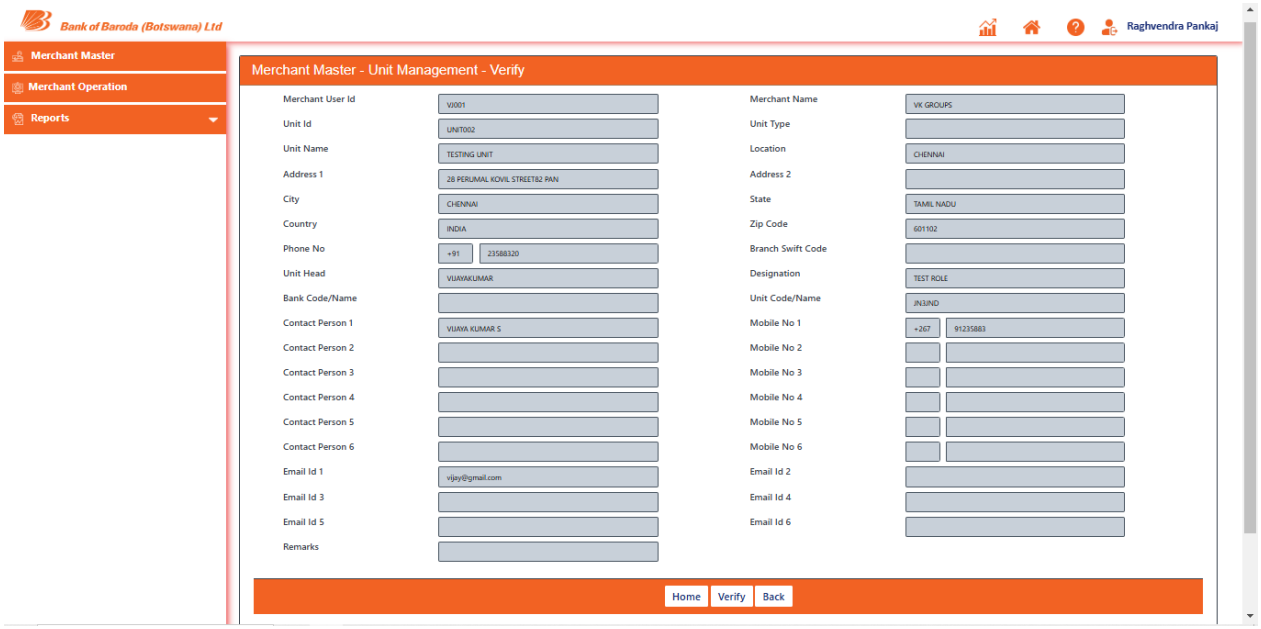
Merchant Master –View Unit Management

Displays the view of the selected record from Unit management.



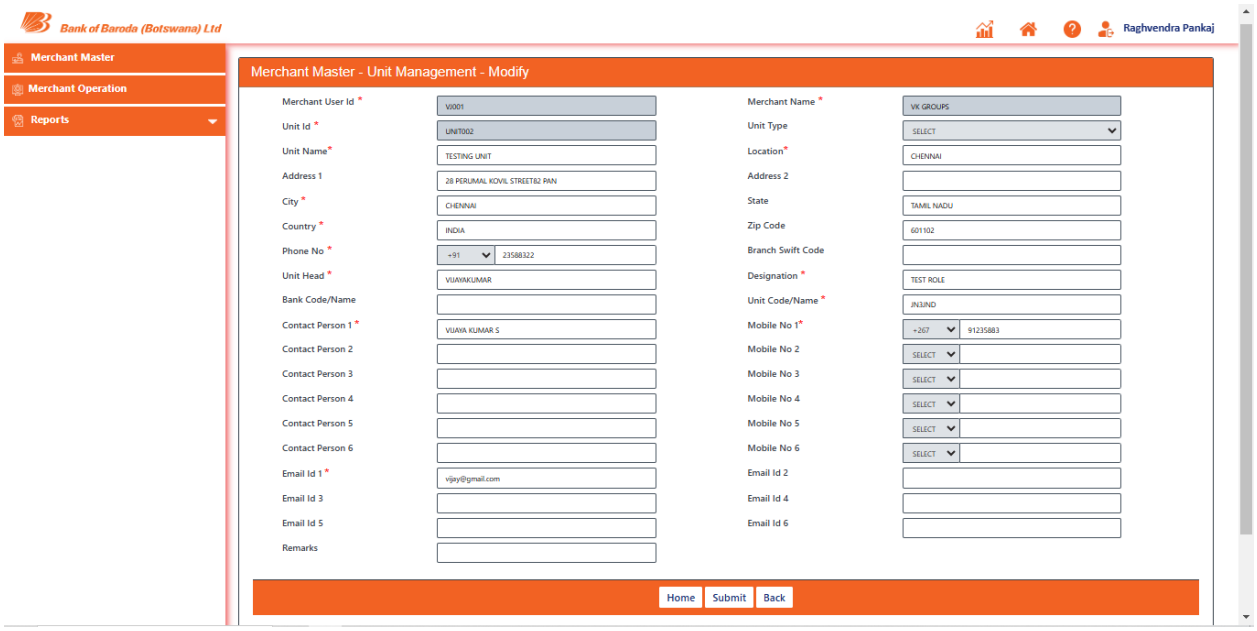
Merchant Master –Verify Unit Management

- Notification parameter verification must be completed on this screen.
- The process involves the maker-checker concept.
- After verification, the status changes to "Verified"



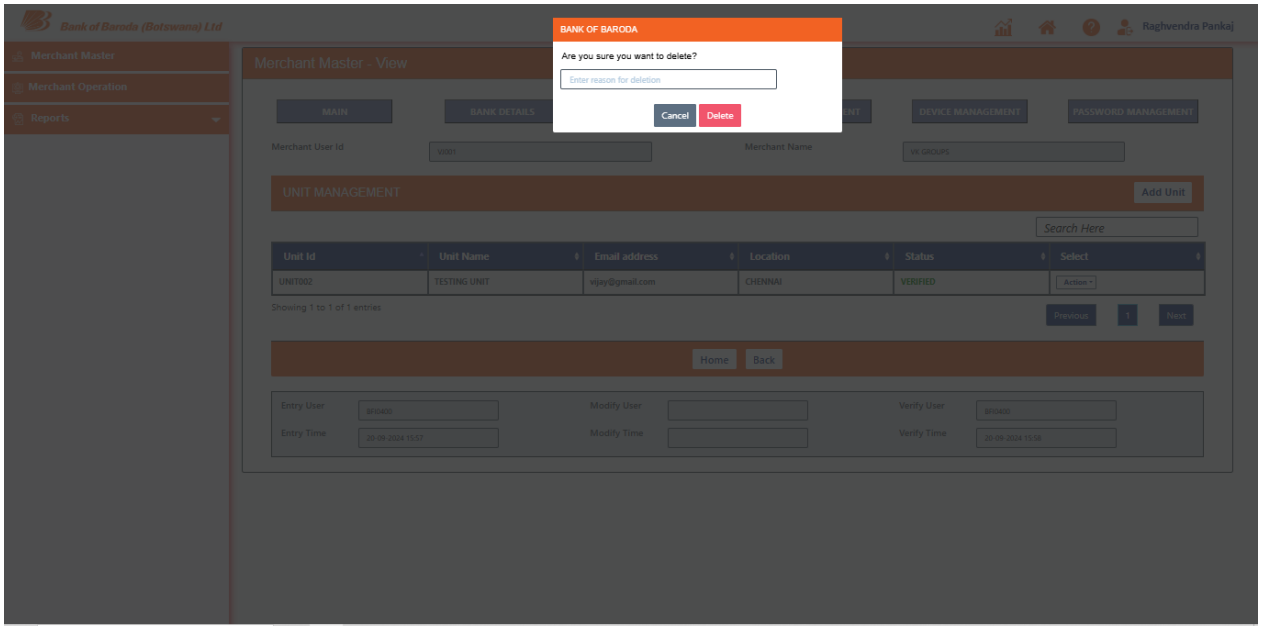
Merchant Master –Modify Unit Management

Modify the fields for the Unit management on this screen. The Screen will appear below,



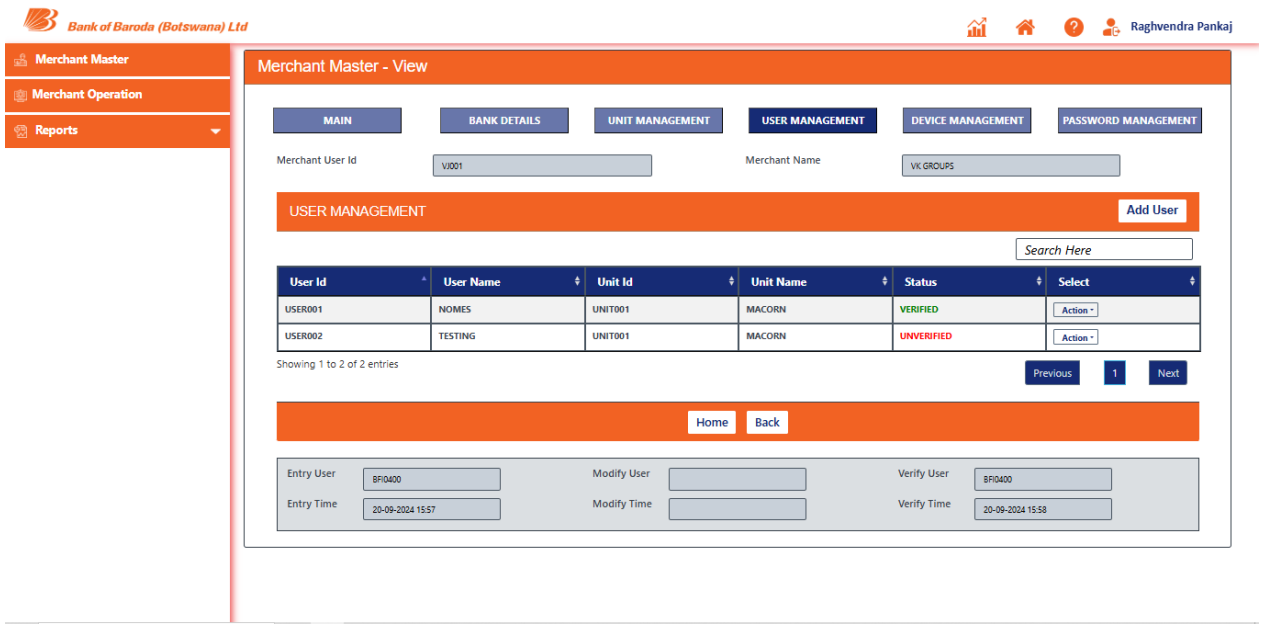
Merchant Master –Delete Unit Management

Displays the Delete of the Unit Management.



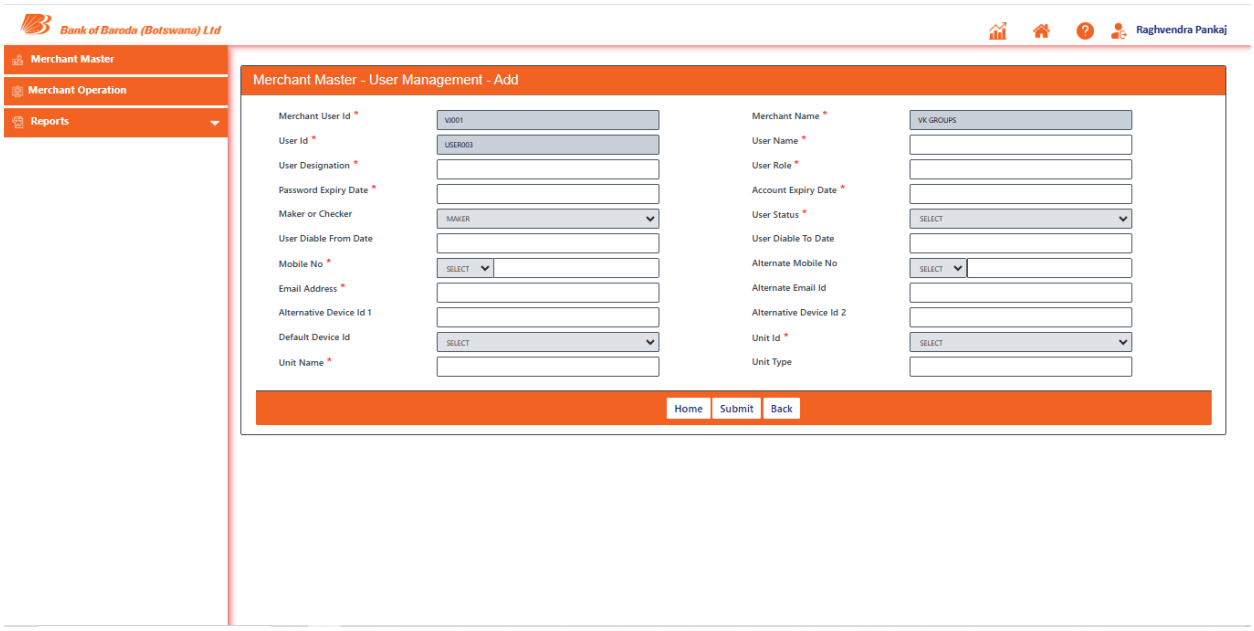
Merchant Master –User Management List

Displays a list of User management. The Screen will appear below,



Merchant Master –Add User Management

- Merchants can manage their users effectively in the user management section.
- Users can be added under the specific merchant currently logged in.
- Counter user details are collected for each user added.
- All mandatory fields must be filled out.
- After filling out the details, the information should be submitted.
- After submitting the user details, the verify status is set to unverified.
- The unverified status requires verification.



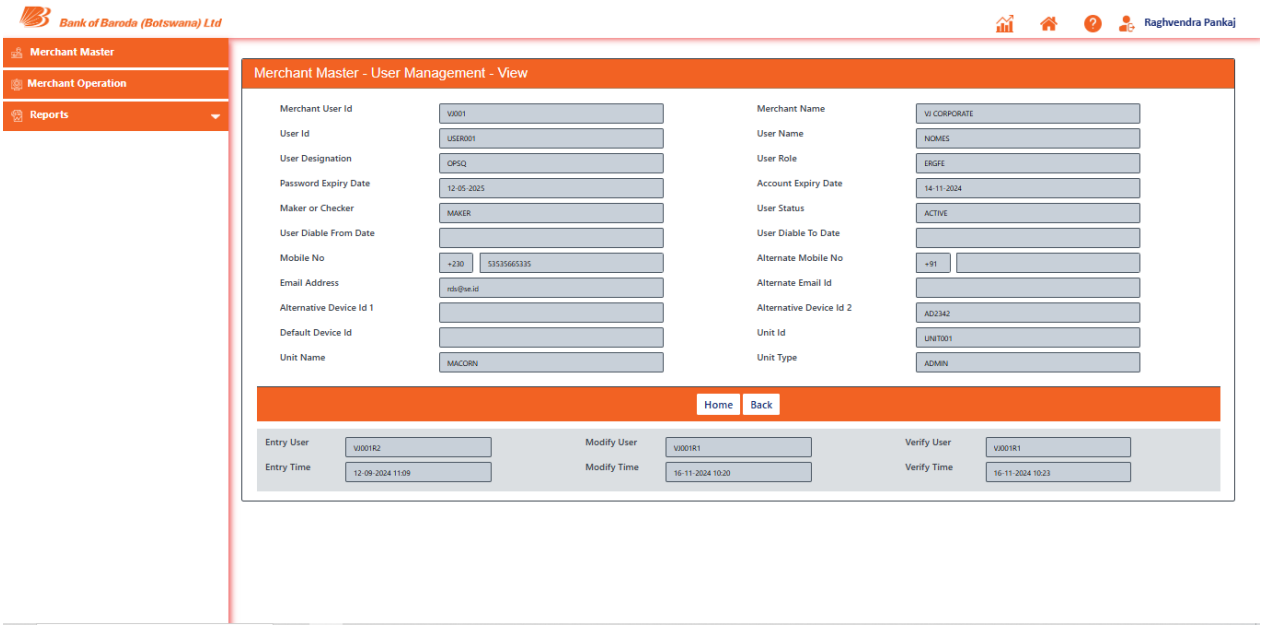
User Management		
Mandatory Field	**User Action**	**Description**
User Id	Displayed	Mandatory Free Text Alphanumeric
User Name	Displayed	Mandatory Free Text Alphanumeric
User Designation	Displayed	Mandatory Free Text Alphanumeric

User Role	Displayed	Mandatory Free Text Alphanumeric
User Status	Displayed	Mandatory Free Text Alphanumeric
Password Expiry Date	Displayed	Mandatory Free Text Alphanumeric

Account Expiry Date	Displayed	Mandatory Free Text Alphanumeric
Maker or Checker	Displayed	Mandatory Free Text Alphanumeric
Mobile Number	Displayed	Mandatory Free Text Alphanumeric
Email Address	Displayed	Mandatory Free Text Alphanumeric
Unit Id	Displayed	Mandatory Free Text Alphanumeric
Unit Name	Displayed	Mandatory Free Text Alphanumeric
Unit Type	Displayed	Mandatory Free Text Alphanumeric

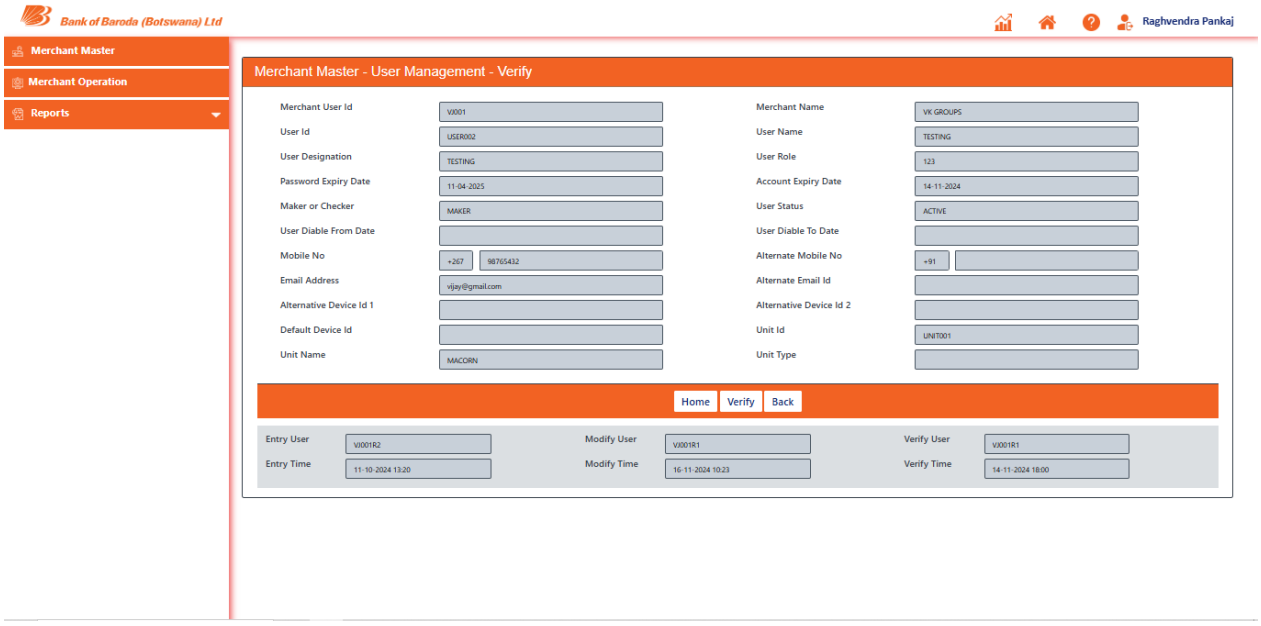
Merchant Master –View User Management

Displays the view of the selected record from User Management



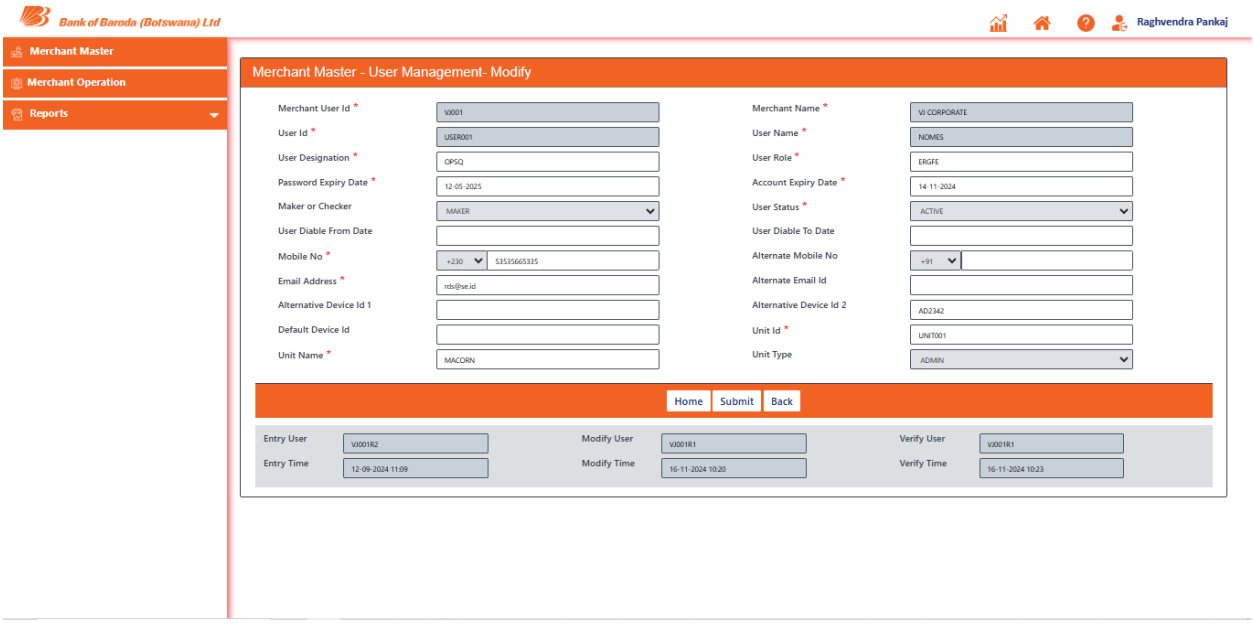
Merchant Master –Verify User Management

- Verify the created user on this screen.
- The created merchant representative cannot verify the counter user.
- Only another representative under the same merchant has the access to verify the counter user.
- After verification, the verify status should change to "verified."



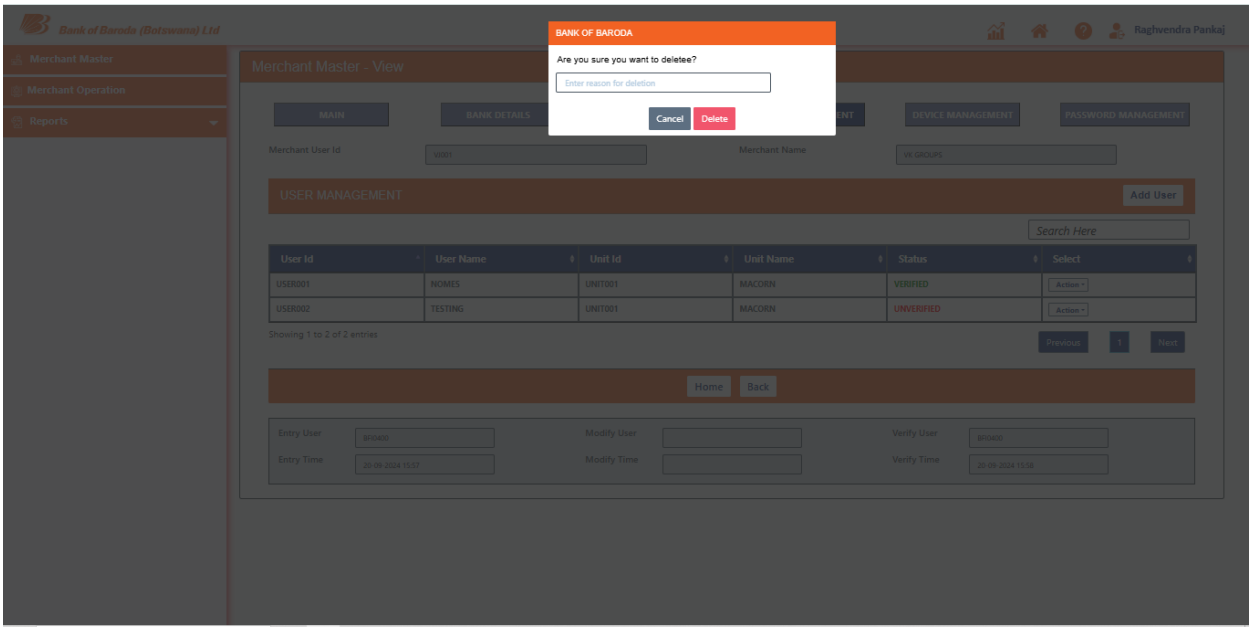
Merchant Master –Modify User Management

- Modify the fields for the user on this screen.
- After modification, the verify status should change to "unverified."
- The user must be verified again after making modifications.



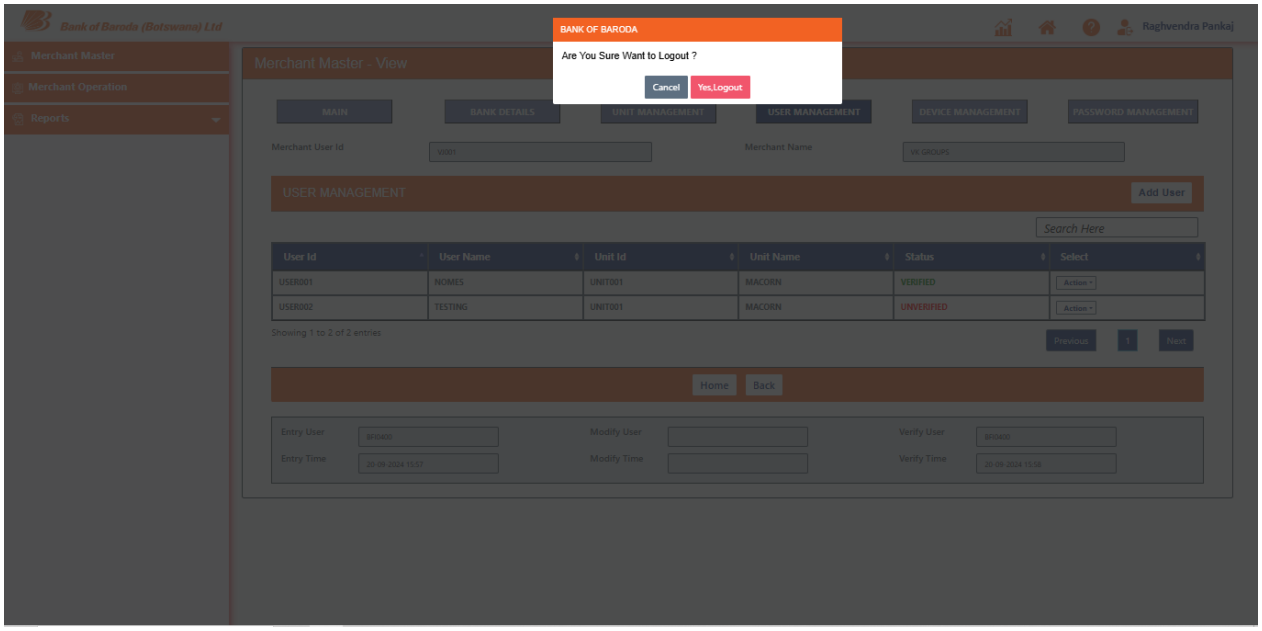
Merchant Master –Delete User Management

Displays the Delete of the User Management.



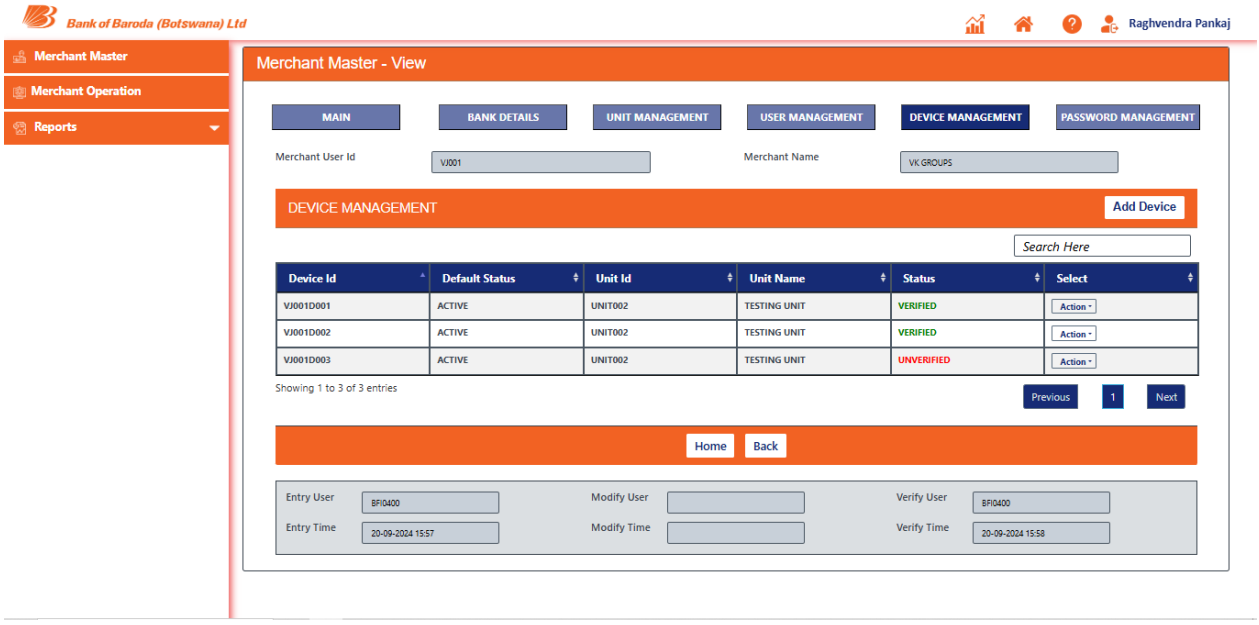
Merchant Master – Reset User management

- When the application is stopped due to a network issue or any other reason, the session remains active, and the logged-in user cannot log in from another device.
- To resolve this, we provide a reset button that allows users to terminate the active session, enabling the same ID to log in on another device.



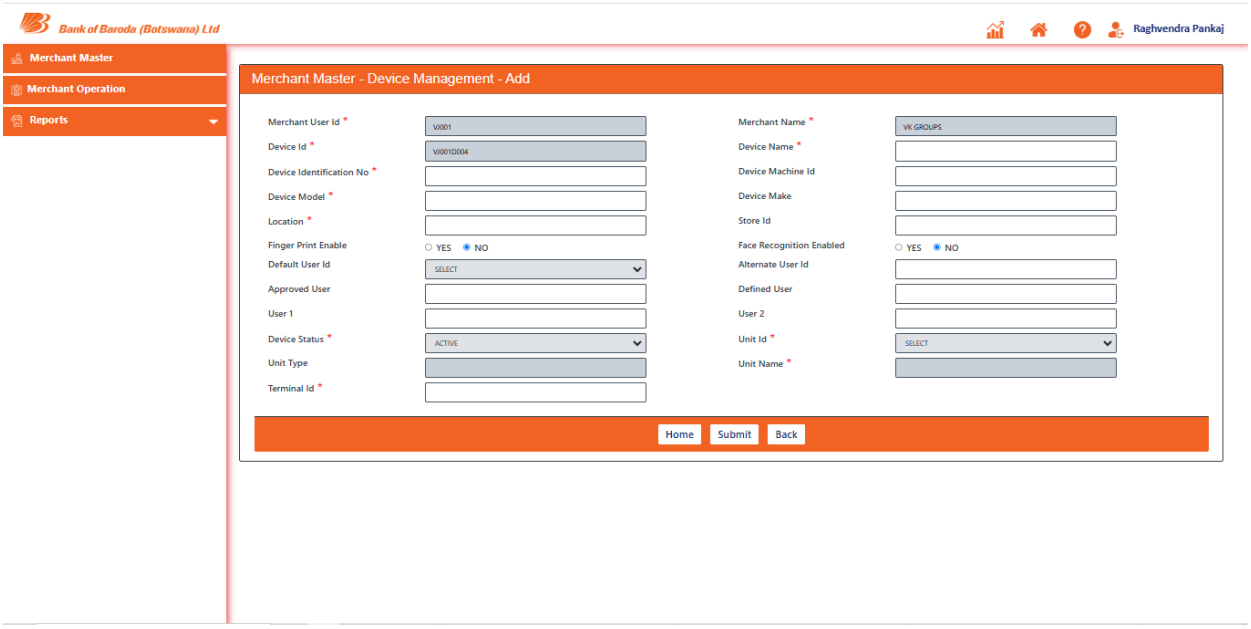
Merchant Master –Device Management List

Displays a list of Notification Parameter. The Screen will appear below,



Merchant Master –Add Device Management

- Merchants can register unique identifiers for each device they possess.
- They can specify which users have permission to utilize each device.
- Functionalities include creating new device IDs.
- All mandatory fields must be filled out.
- Information should be submitted after filling out the details.
- The verify status is set to unverified after submission.
- The unverified status requires verification.



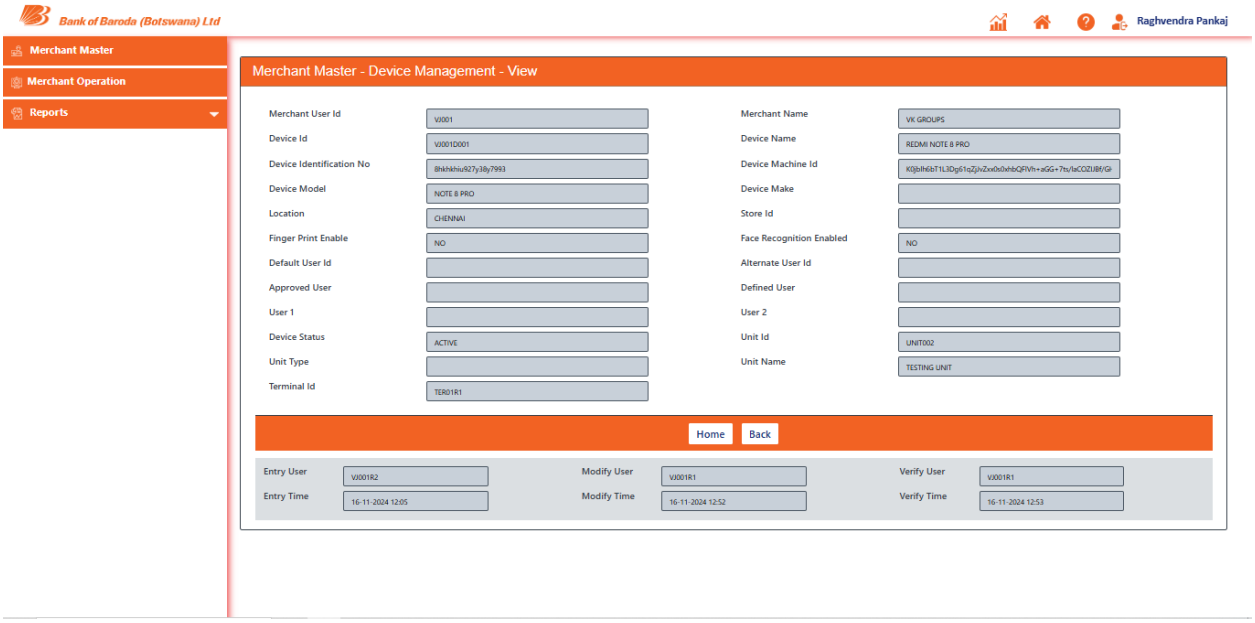
Device Management		
Mandatory Field	**User Action**	**Description**
Device Id	Displayed	Mandatory Free Text Alphanumeric
Device Name	Displayed	Mandatory Free Text Alphanumeric

Device Model	Displayed	Mandatory Free Text Alphanumeric
Device Identification No	Displayed	Mandatory Free Text Alphanumeric
Device Machine Id	Displayed	Mandatory Free Text Alphanumeric
Location	Displayed	Mandatory Free Text Alphanumeric

Store Id	Displayed	Mandatory Free Text Alphanumeric
Terminal Id	Displayed	Mandatory Free Text Alphanumeric
Device Status	Displayed	Mandatory Free Text Alphanumeric
Unit Id	Displayed	Mandatory Free Text Alphanumeric
Unit Type	Displayed	Mandatory Free Text Alphanumeric
Unit Name	Displayed	Mandatory Free Text Alphanumeric

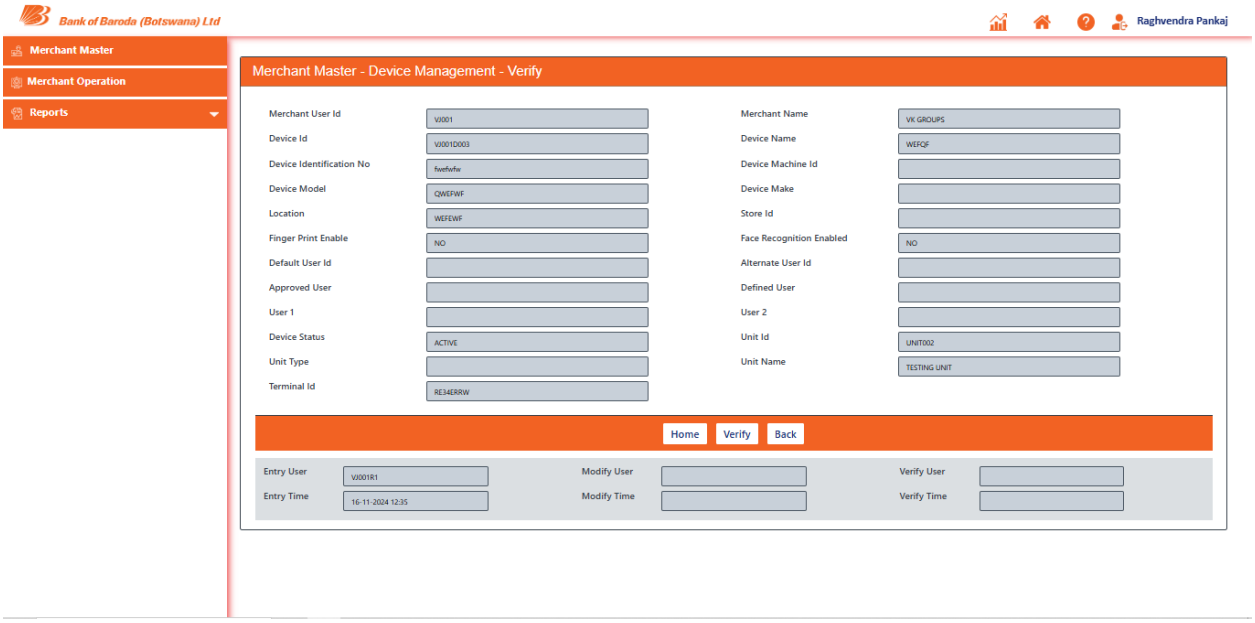
Merchant Master –View Device Management

Displays the view of the selected record from Device Management



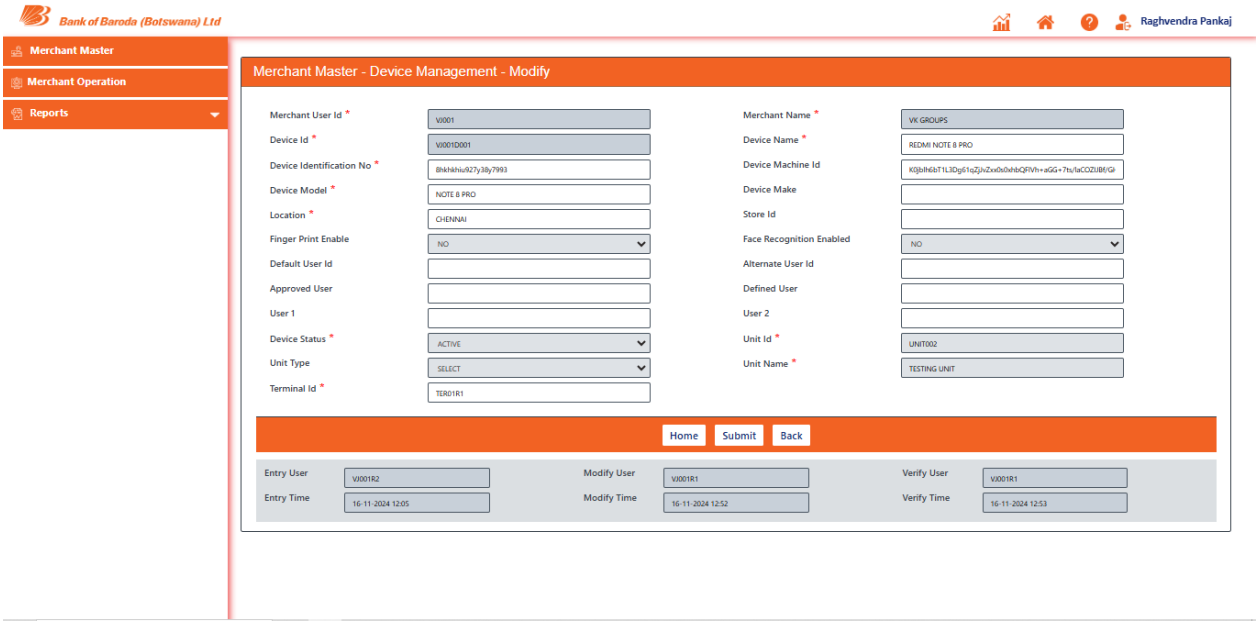
Merchant Master –Verify Device Management

- Verify the created device on this screen.
- The created merchant representative cannot verify the device.
- Only another representative under the same merchant has the access to verify the device.
- After verification, the verify status should change to "verified."



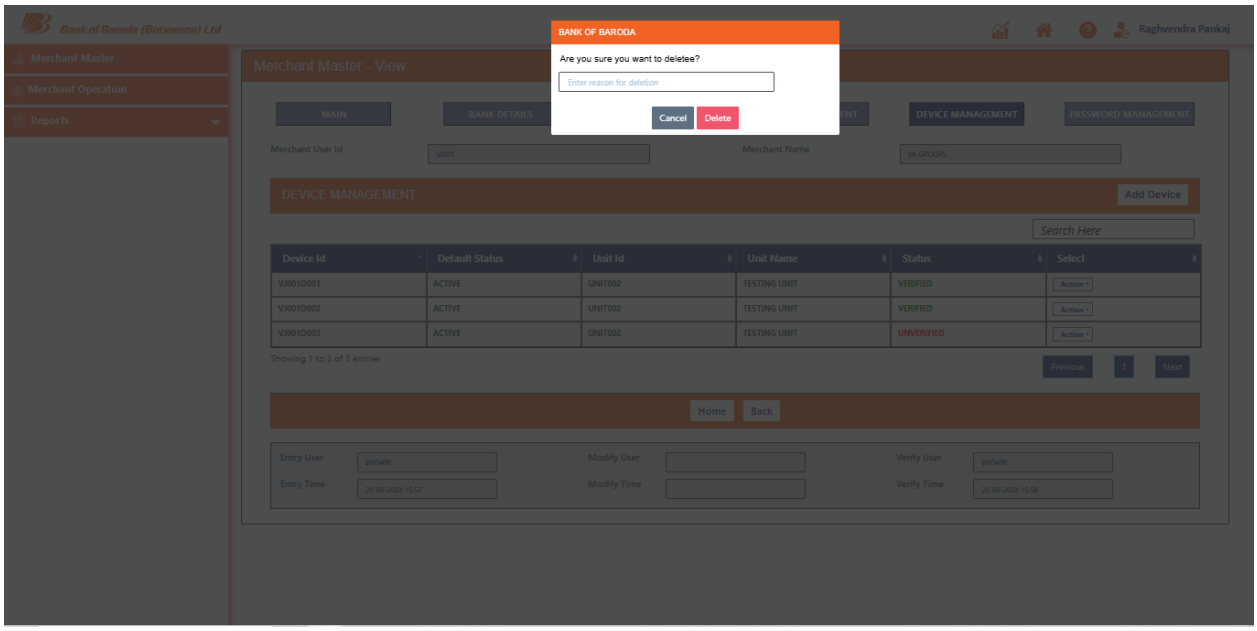
Merchant Master –Modify Device Management

- Modify the fields for the device on this screen.
- After modification, the verify status should change to "unverified."
- The device must be verified again after making modifications.
- An option to delete the device is also available.



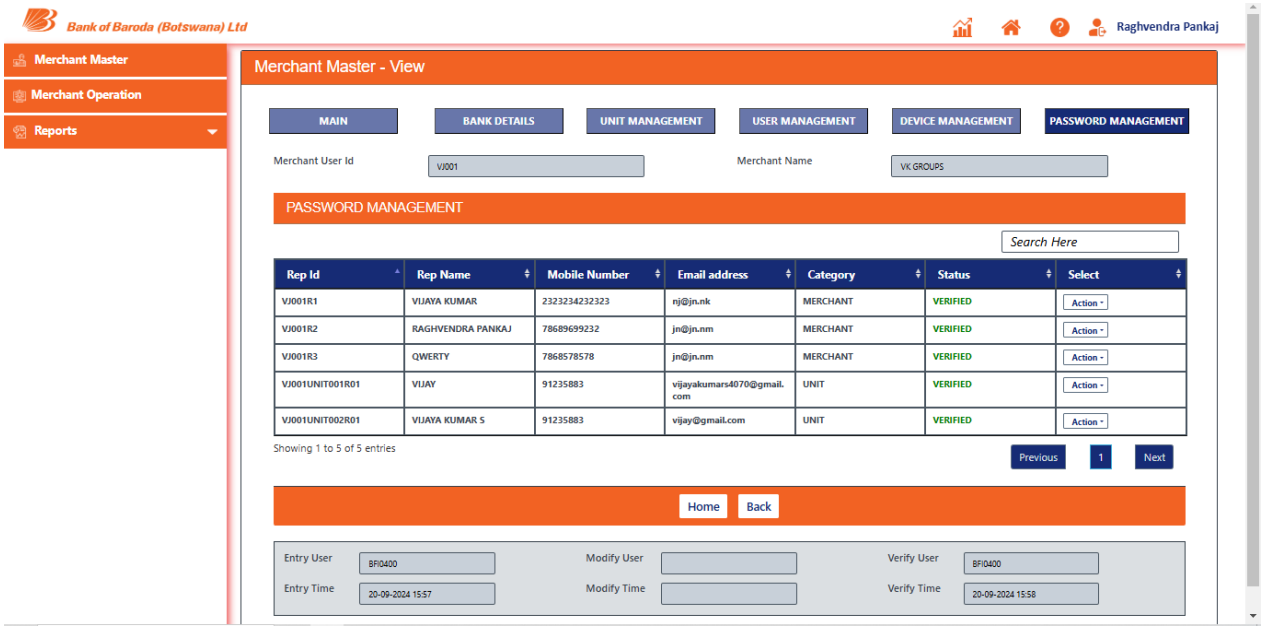
Merchant Master –Delete Device Management

Displays the Delete of the Device Management.



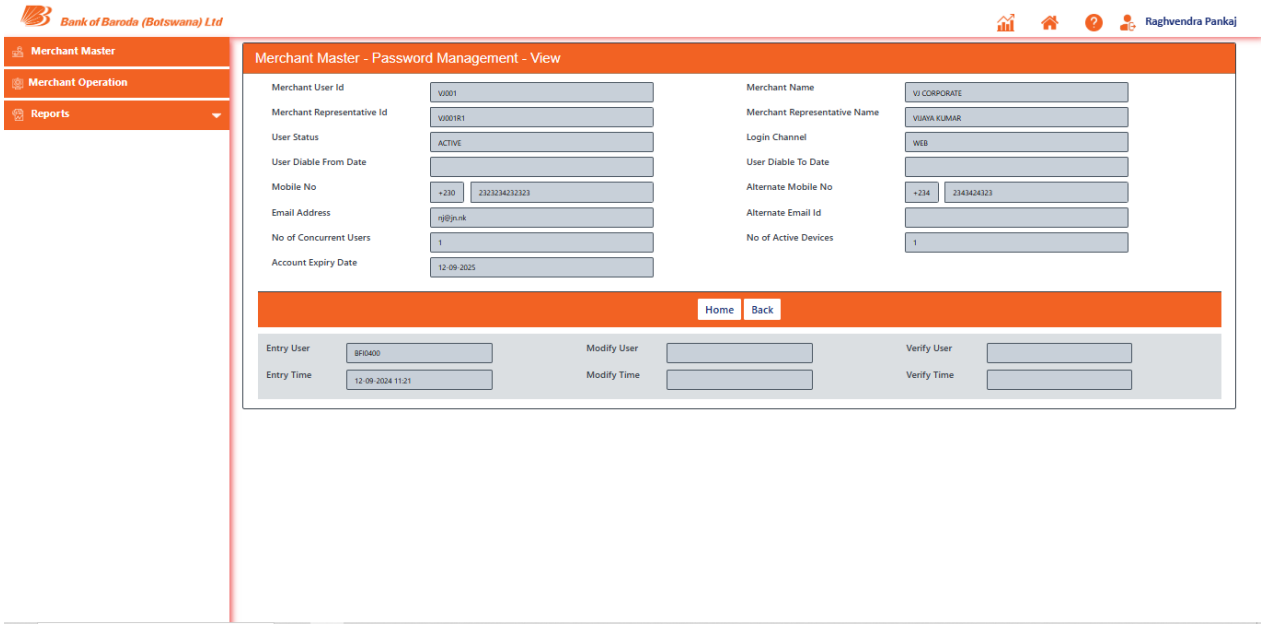
Merchant Master –Password Management List

Displays a list of Notification Parameter. The Screen will appear below,



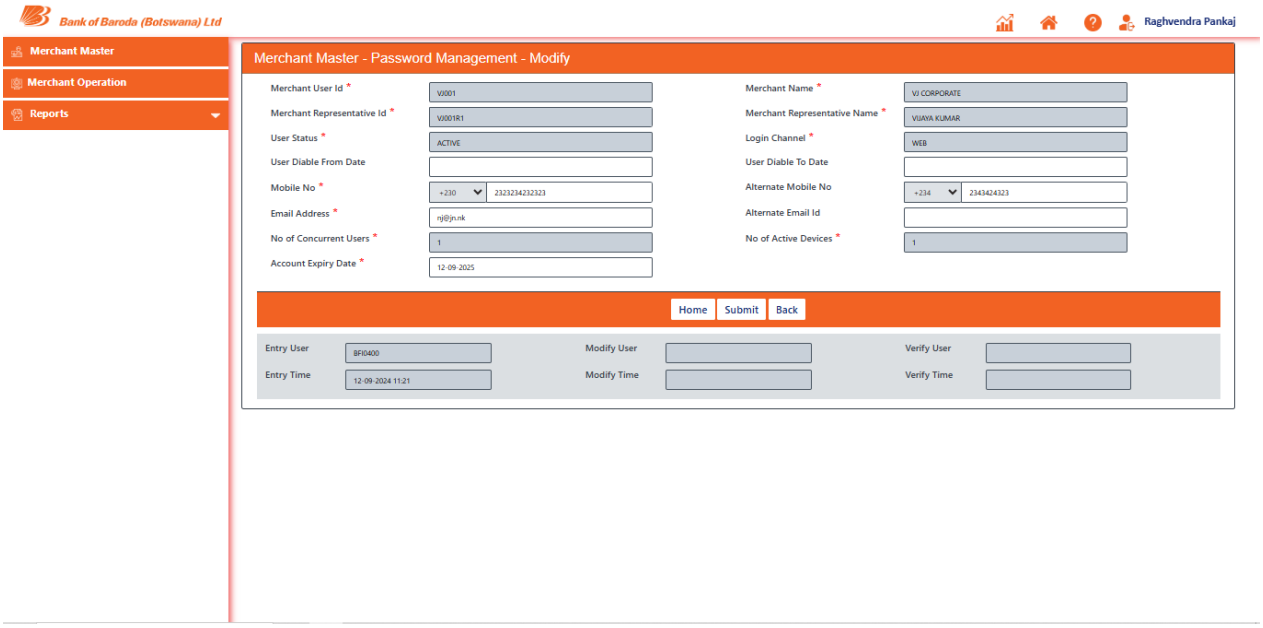
Merchant Master –View Password Management

Displays the view of the selected record from Notification parameter. The Screen will appear below,



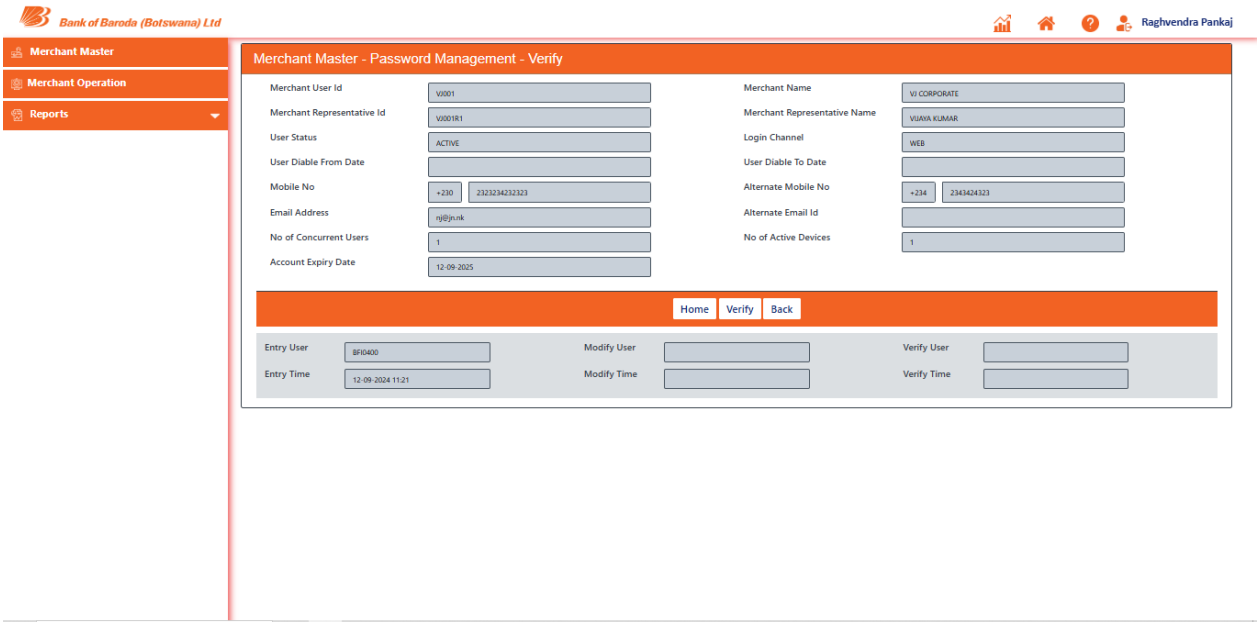
Merchant Master –Modify Password Management

Modify the fields for the Password Management on this screen.The Screen will appear below,



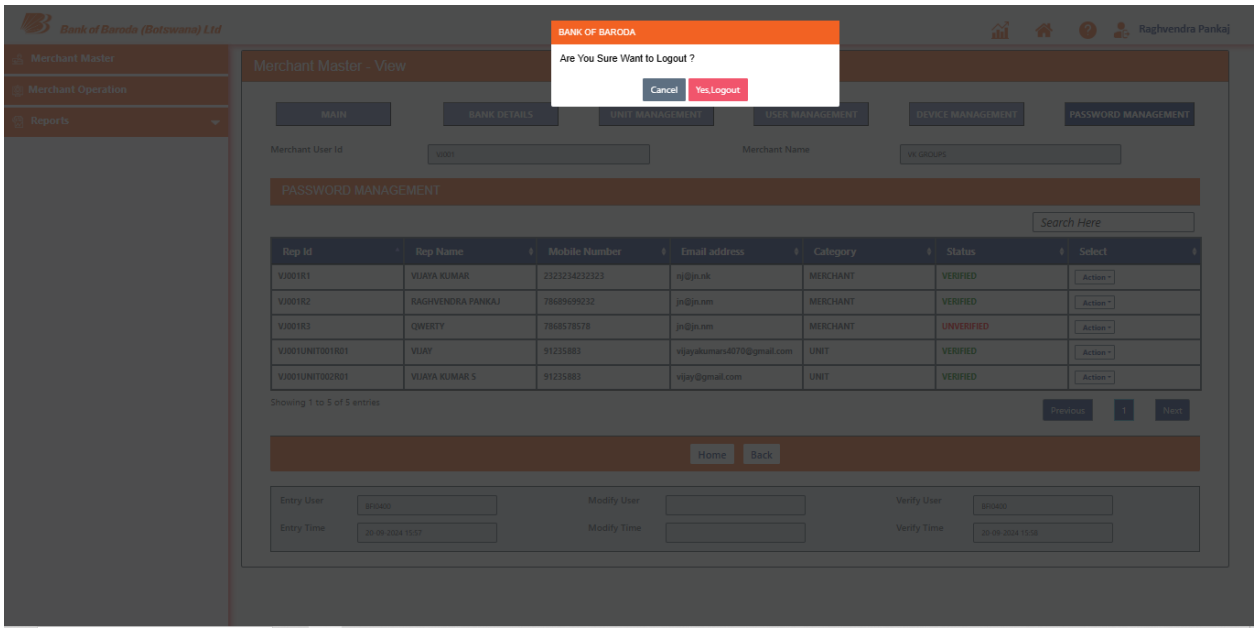
Merchant Master –Verify Password Management

- Settlement account verification must be completed on this screen.
- The process involves the maker-checker concept.
- After verification, the status changes to "Verified"



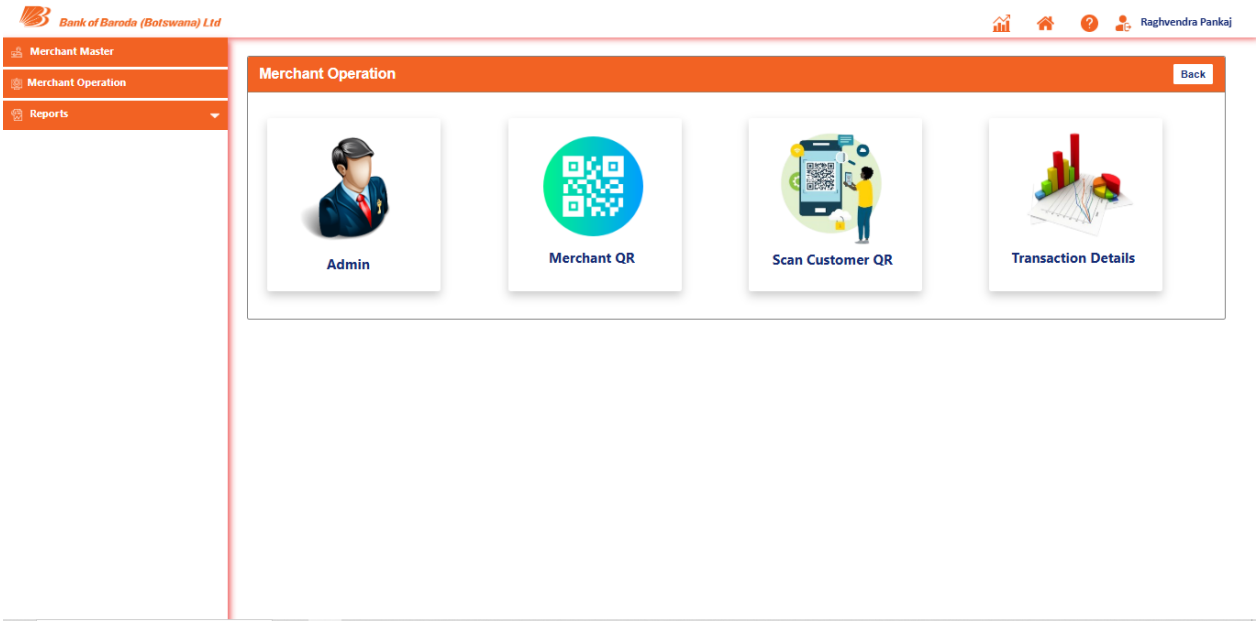
Merchant Master – Reset Password management

- When the application is stopped due to a network issue or any other reason, the session remains active, and the logged-in user cannot log in from another device.
- To resolve this, we provide a reset button that allows users to terminate the active session, enabling the same ID to log in on another device.



2.2. Merchant Operations

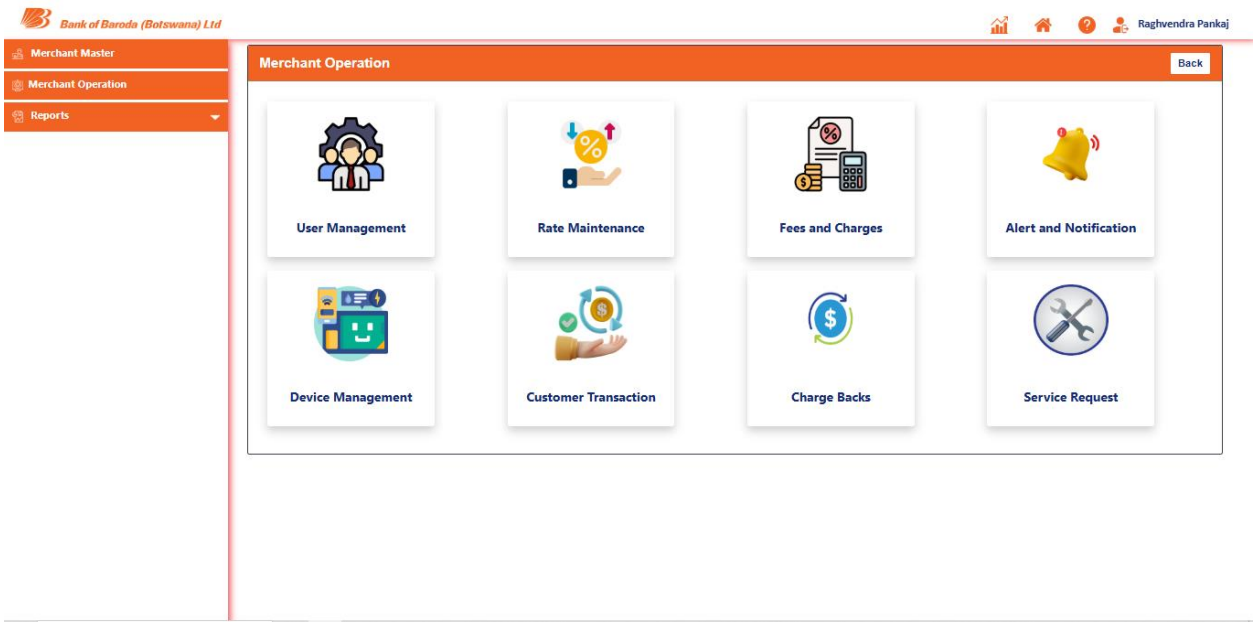
- Admin
- Merchant QR
- Customer QR
- Transaction Details



2.2.1. Admin Operations

In the admin module, we have several management functionalities including

- User Management
- Device Management
- Rate Maintenance
- Customer Transactions
- Fees and Charges
- Charge Backs
- Alert and Notification
- Service Request

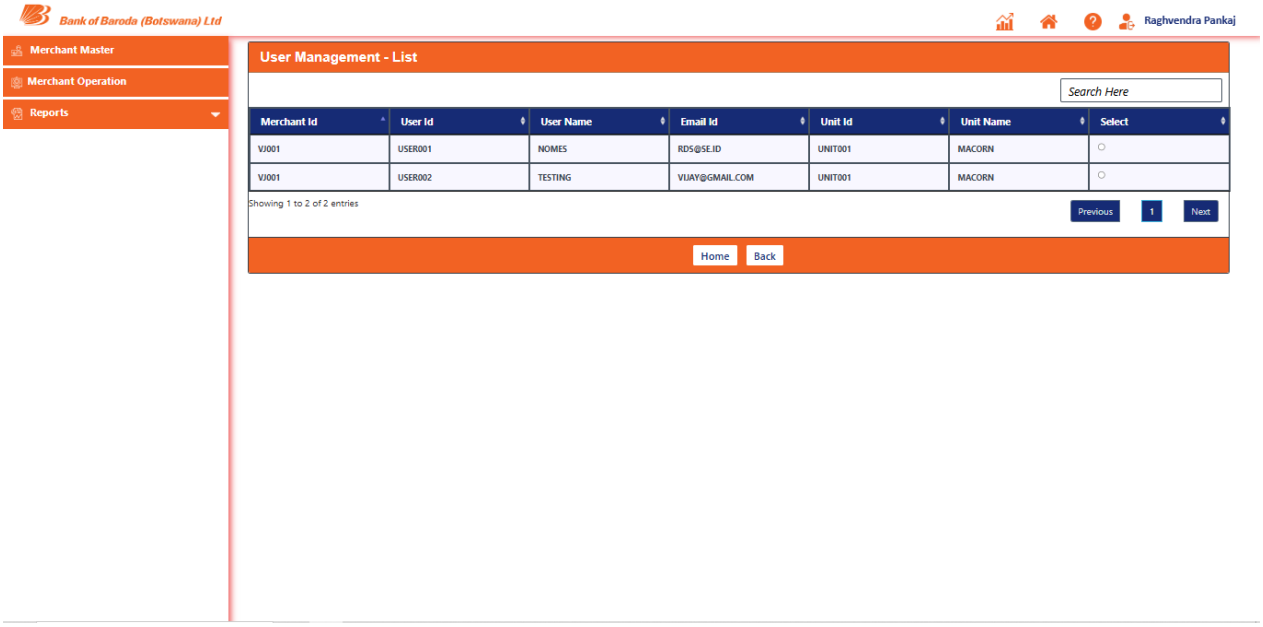


2.2.1.1. User Management

In the user management section, merchants have the capability to manage their users effectively. This includes functionalities such as creating new user accounts, updating existing user information, verifying user details, and modifying user permissions as needed.

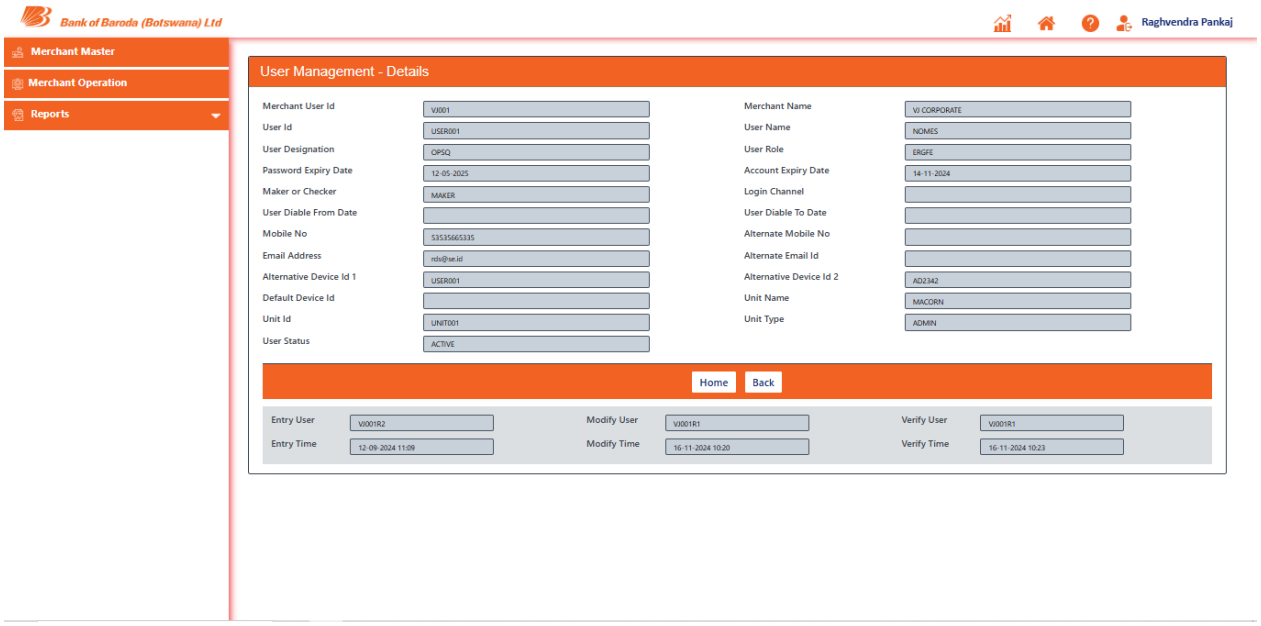
User Management –List

Displays a list of already created users. The Screen will appear below,



User Management –View

To display the View Screen. The Screen will appear below,

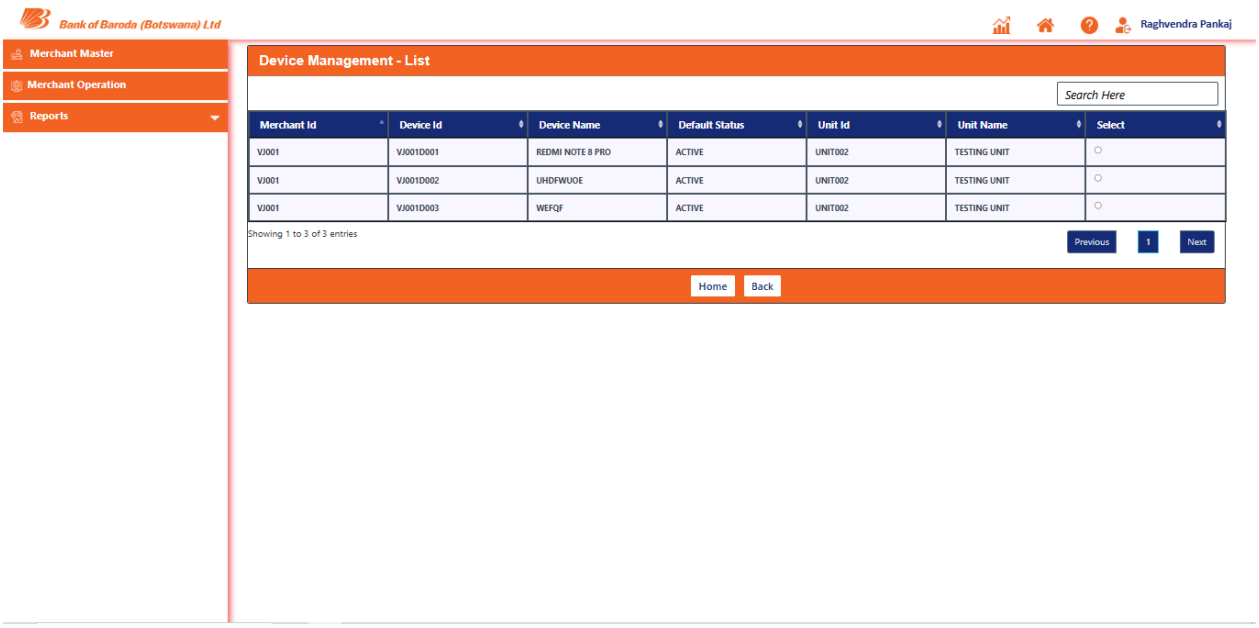


2.2.1.2. Device Management

- Merchants can register unique identifiers for each device they possess.
- They can specify which users have permission to use each device.
- Functionalities include: creating new device id, updating users who can access, verify, and modify permissions as needed.

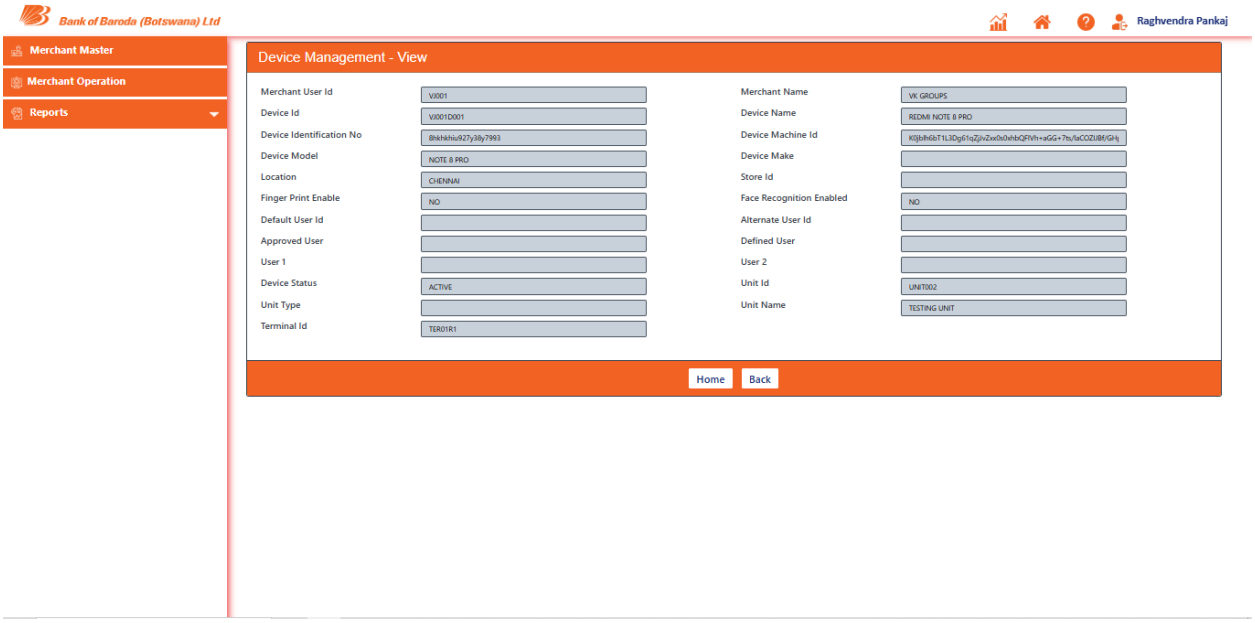
Device Management –List

Displays a list of Device management. The Screen will appear below,



Device Management –View

Displays the view of the selected record from Notification parameter. The Screen will appear below,

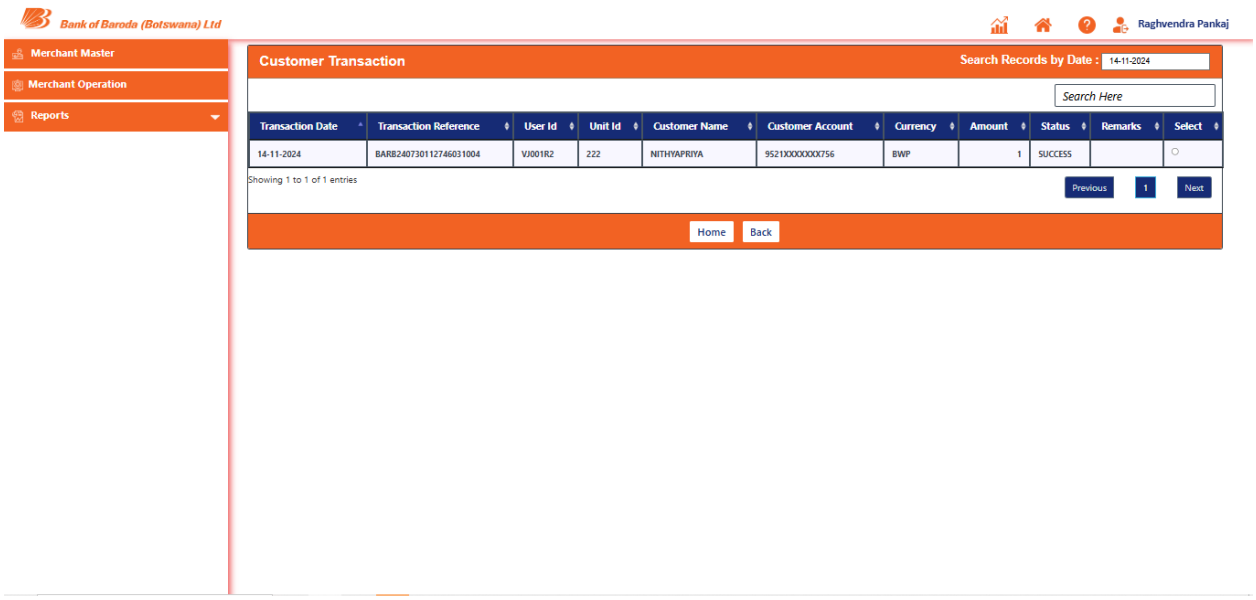


2.2.1.3. Customer Transactions

A transaction list provides the details of all transactions conducted within a specified timeframe or across a certain period. Transaction list typically includes message reference, audit reference, date and time, bank, beneficiary account, status, currency, amount.

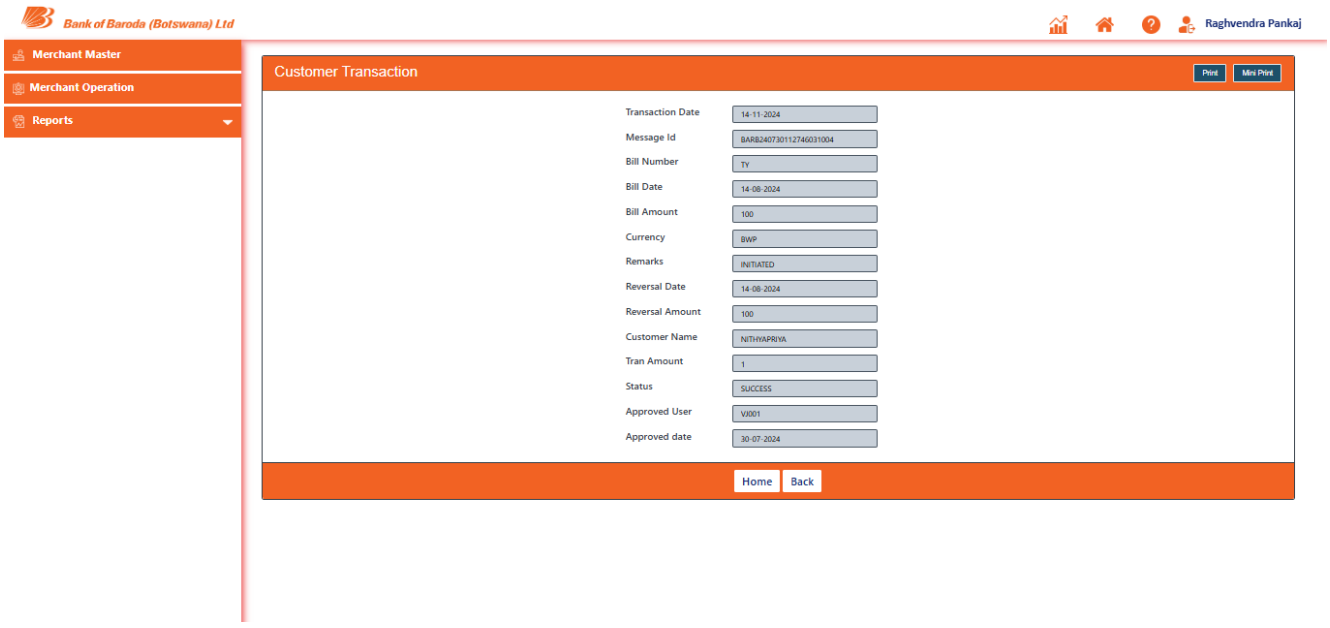
Customer Transactions –List

Display the list of Customer transactions. The Screen will appear below,



Customer Transactions –View

Display the View of Customer transaction. The Screen will appear below,

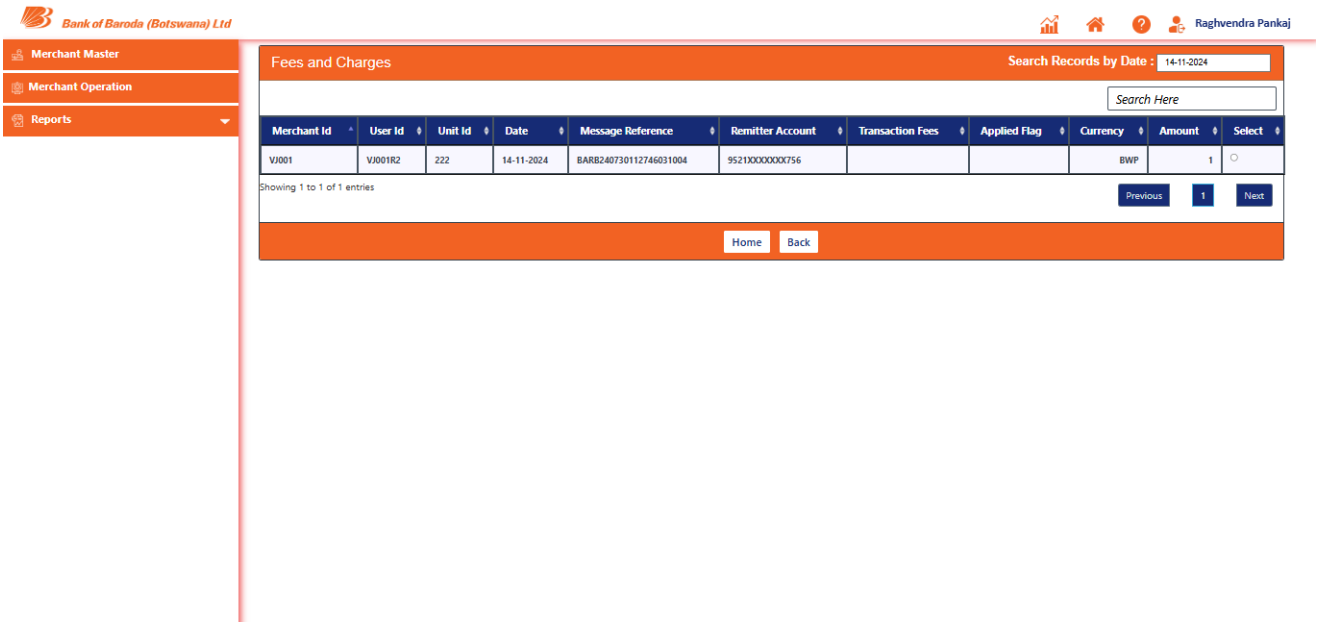


2.2.1.4. Fees and Charges

- In addition to service charges, merchants may incur additional charges and fees depending on their agreement with the bank or payment processor.
- These charges could include setup fees, monthly or annual subscription fees, chargeback fees (fees incurred when a customer disputes a transaction), and other miscellaneous fees.
- The specific fees and charges vary depending on the terms of the merchant's agreement and the services they require.

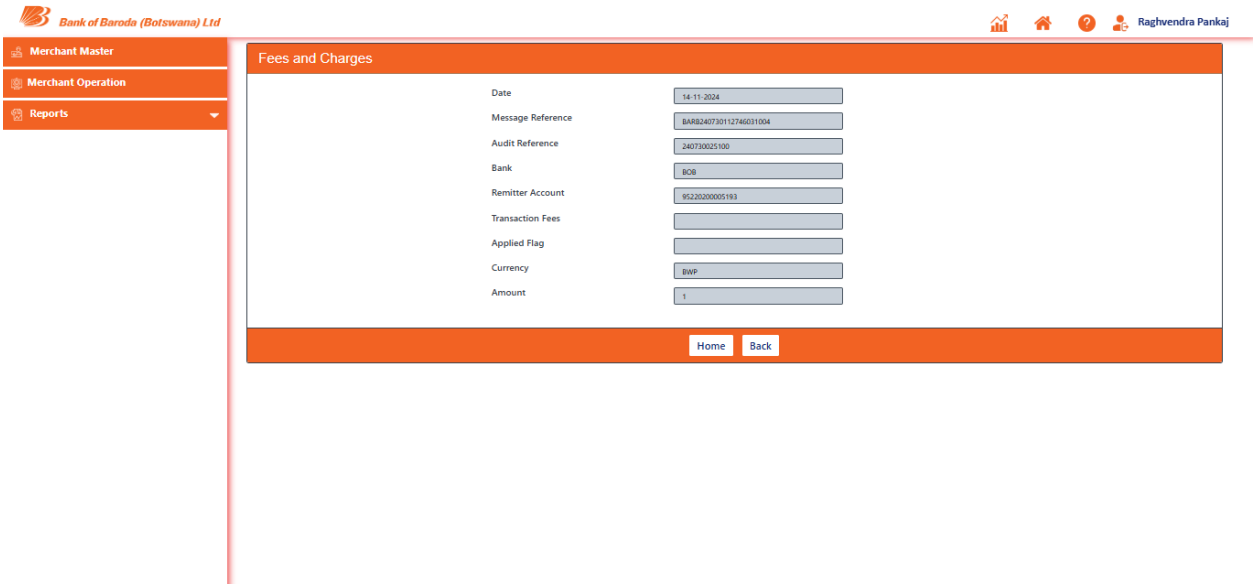
Fees and Charges –List

Display the list of Fees and Charges. The Screen will appear below,



Fees and Charges –View

Display the View of Fees and charges. The Screen will appear below,

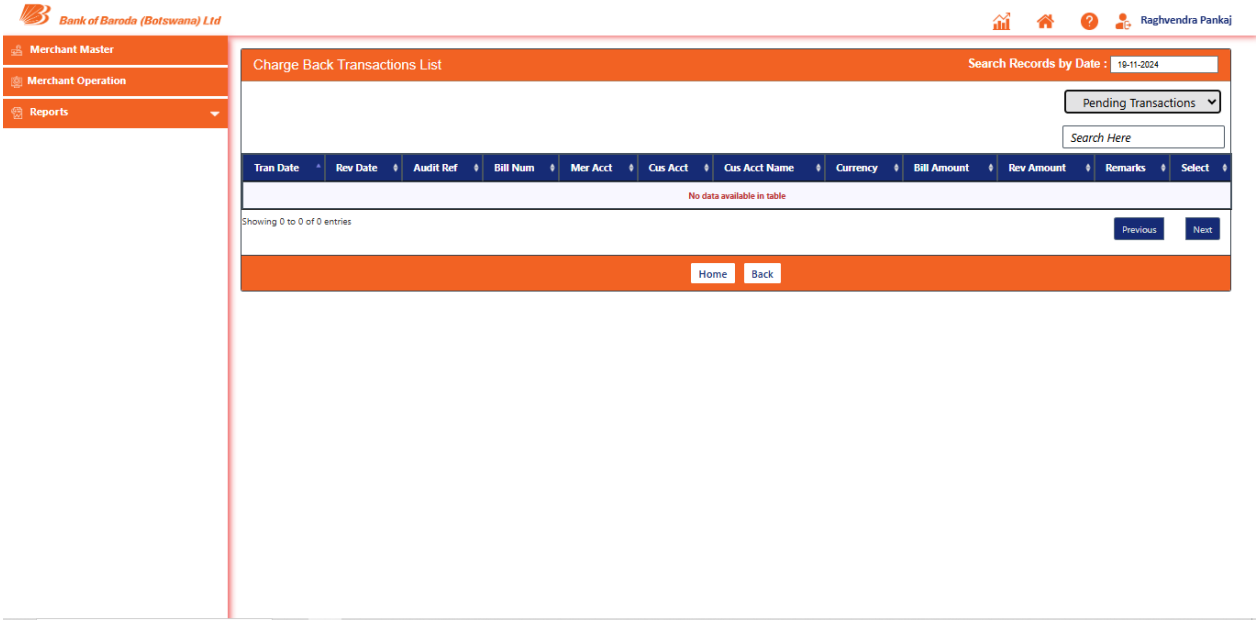


2.2.1.5. Charge Backs

- The chargeback module facilitates transaction approvals.
- It provides a comprehensive view of transaction statuses, including: Pending transaction, Reverted transaction, Initiated transaction and All transaction
- Users can filter transactions by selecting a specific date.
- There is an option to download filtered transaction lists for analysis or record-keeping.
- This functionality streamlines chargeback management by offering clear insights into transaction statuses.
- It supports efficient approval and reporting processes.

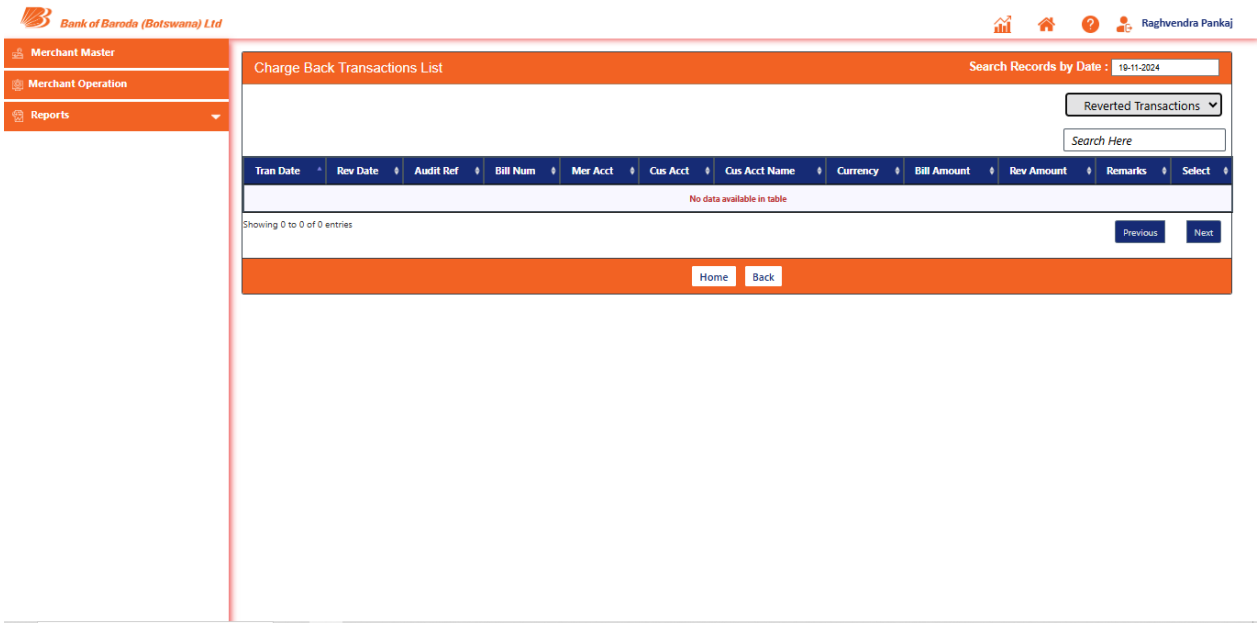
Charge Backs –Pending Transaction

- Chargeback in this list are awaiting further processing.
- These are Chargeback that have been initiated but not yet finalized.
- In this stage, you have the option to revert the Chargeback if necessary, possibly due to errors or disputes.



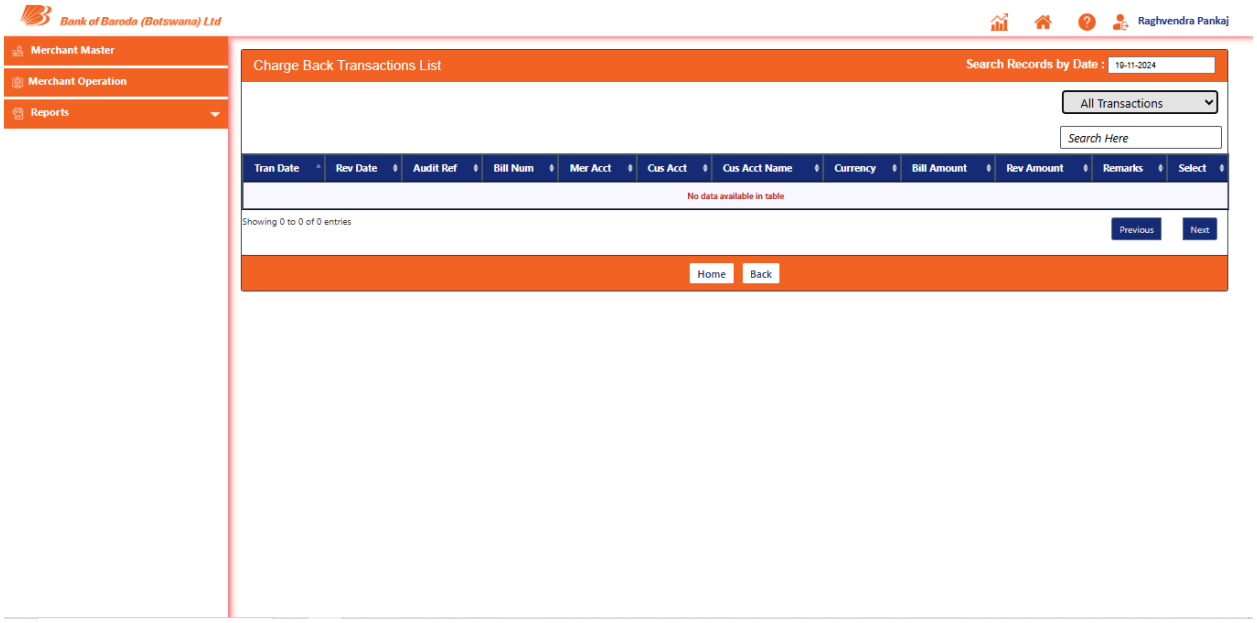
Charge Backs –Reverted Transaction

- If a Chargeback from the Pending list is reverted, it gets moved to the Reverted list.
- The Reverted list contains all Chargeback that have been reversed or canceled during the chargeback process.
- This list serves as a record of all Chargeback that were not successfully processed or were intentionally reversed.



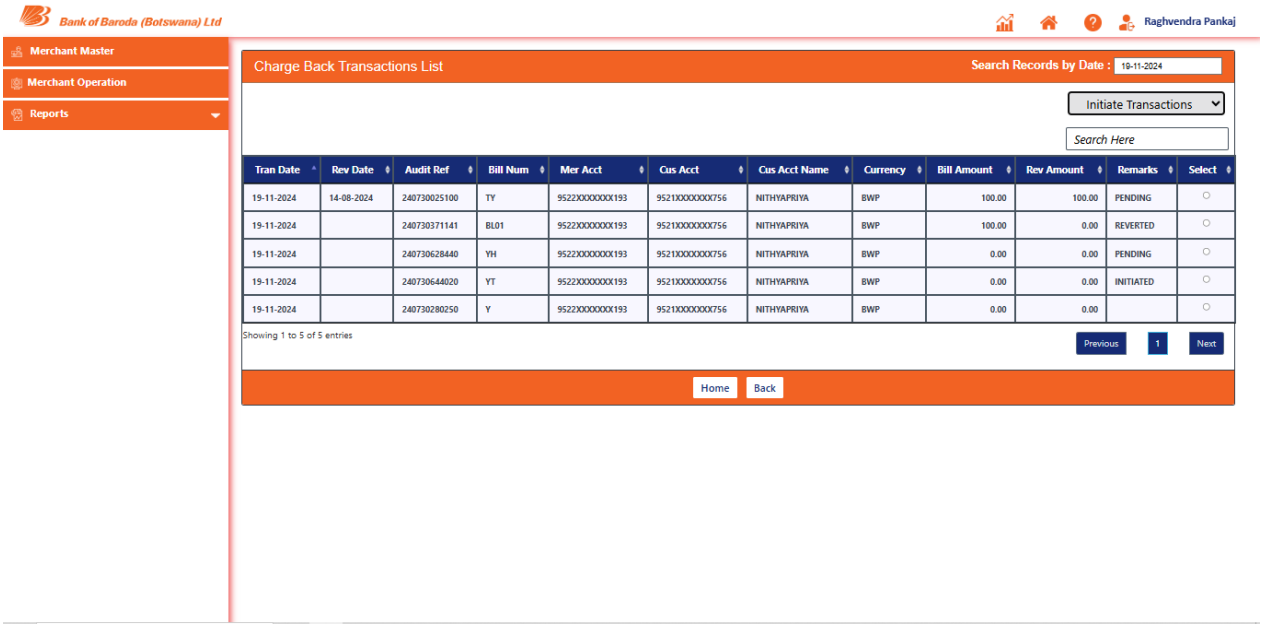
Charge Backs –All Transaction

- The All Chargeback list provides a comprehensive view of both pending and reverted Chargeback.
- This list is used for tracking and reviewing the status of all Chargeback that have been processed, whether they were completed, pending, or reverted.
- It offers a complete overview, making it easier to manage and audit the chargeback process.



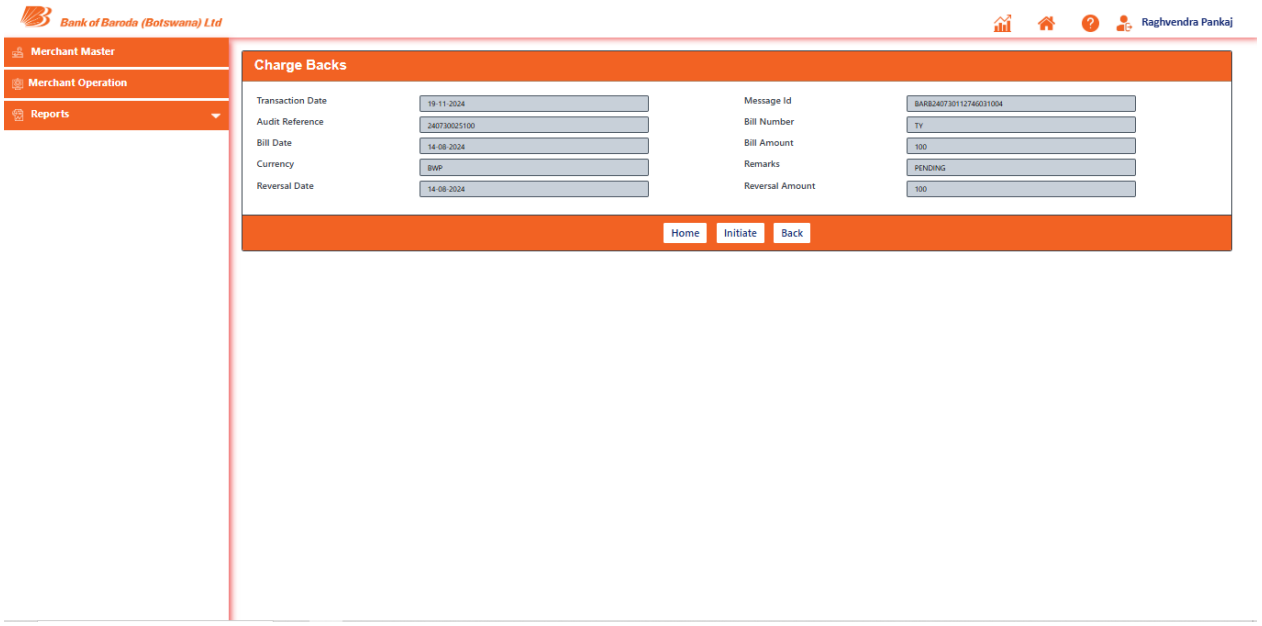
Charge Backs –Initiated Transaction

- On this screen, We initiate the chargeback.
- After initiation, the record needs to be approved.
- The record is moved to the pending list, where the approval function is available.



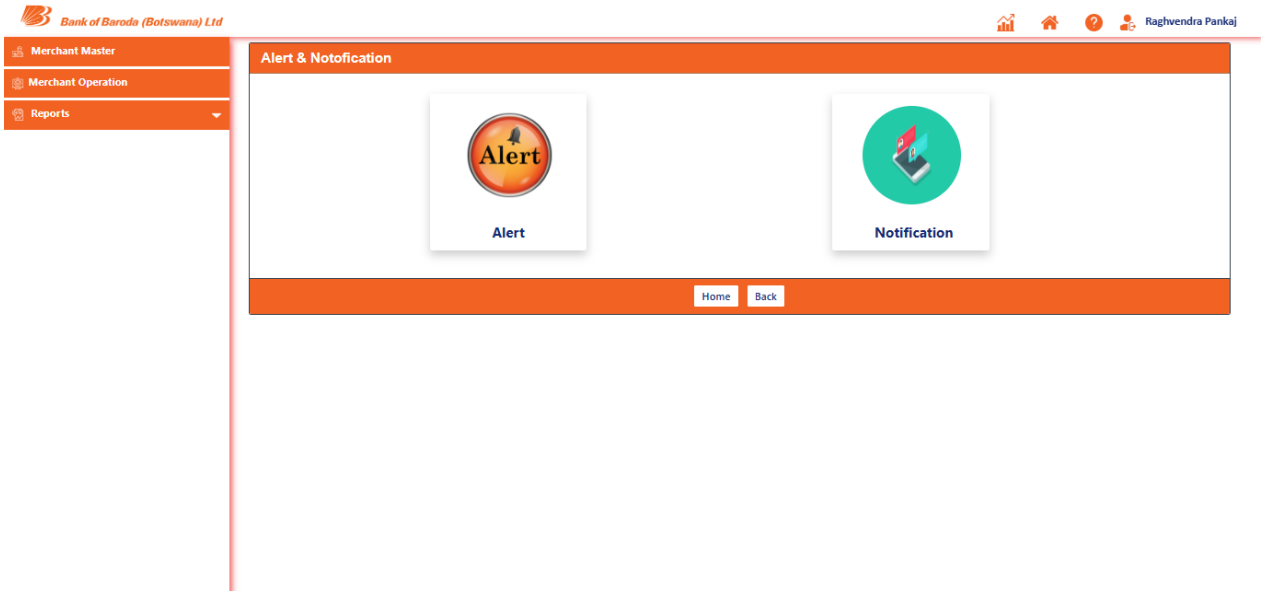
Initiated Transaction –View

Display the View of Initiated Transaction. The Screen will appear below,



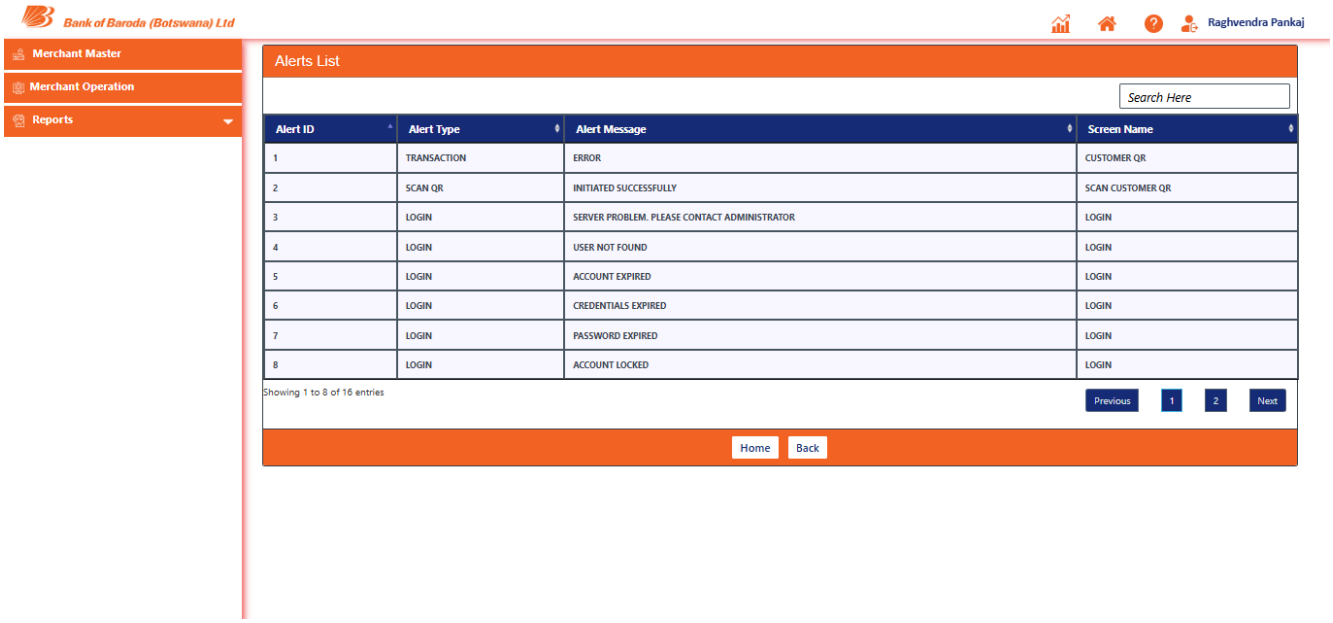
2.2.1.6. Alert and Notification

- It refers to settings that govern how merchants receive notifications or alerts regarding their transactions and account activities.
- These parameters allow merchants to customize their notification preferences based on their preferences and business needs.
- Notifications can include alerts for successful transactions, failed transactions, chargebacks, account balance updates, suspicious activities, and more.
- Merchants can choose to receive notifications via email, SMS, mobile app notifications, or through a dedicated merchant portal.



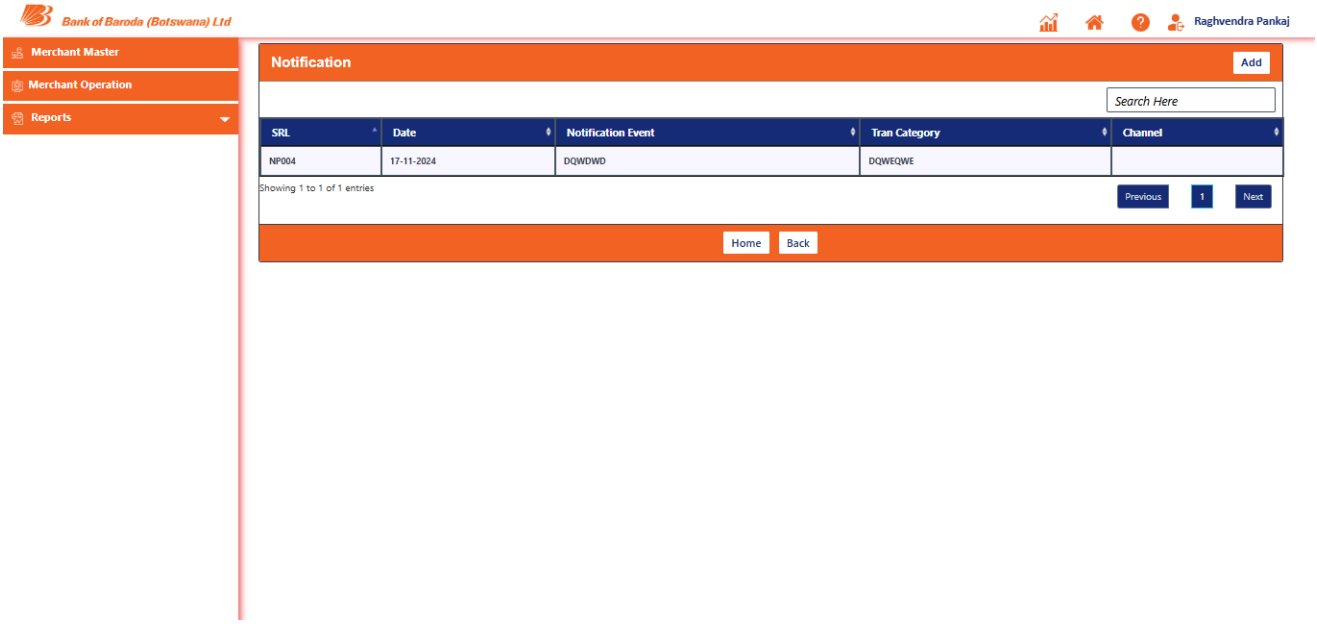
Alerts

Display the list of Alerts. The Screen will appear below,



Notification

- Displays a list of notifications.
- Notifications can include: Successful transactions, Failed transactions, Chargebacks, Account balance updates, Suspicious activities, Other relevant updates.

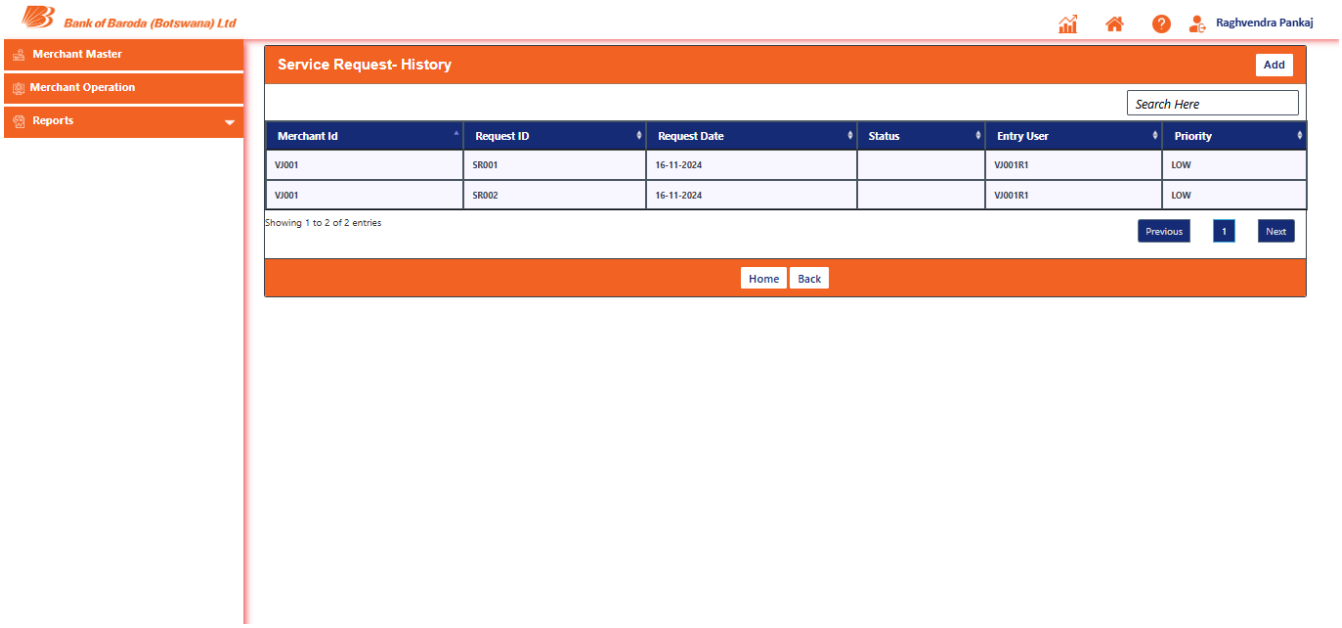


2.2.1.7. Service Request

- Merchants can raise service requests to the bank user if they encounter any issues or require assistance.
- It refers to a formal or informal inquiry, request, or application made by a customer or account holder to the bank for a specific service or action. These requests can encompass a wide range of banking activities and services.

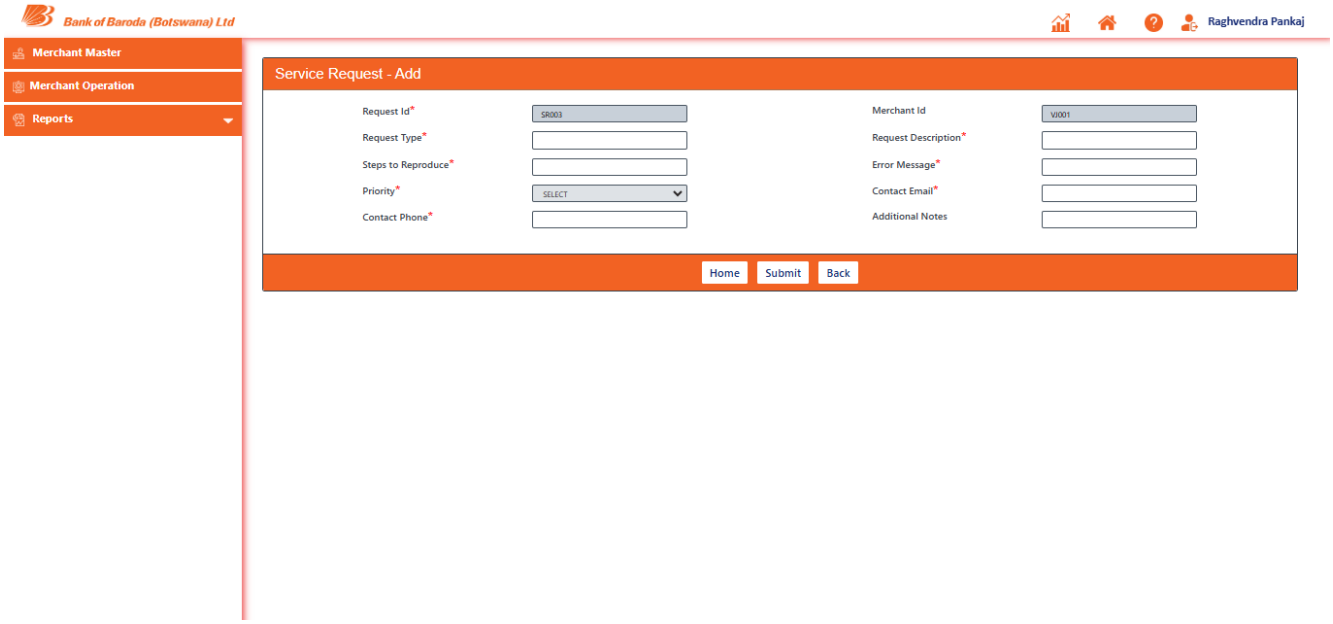
Service Request-List

Display the list of Service. The Screen will appear below,



Service Request -Add

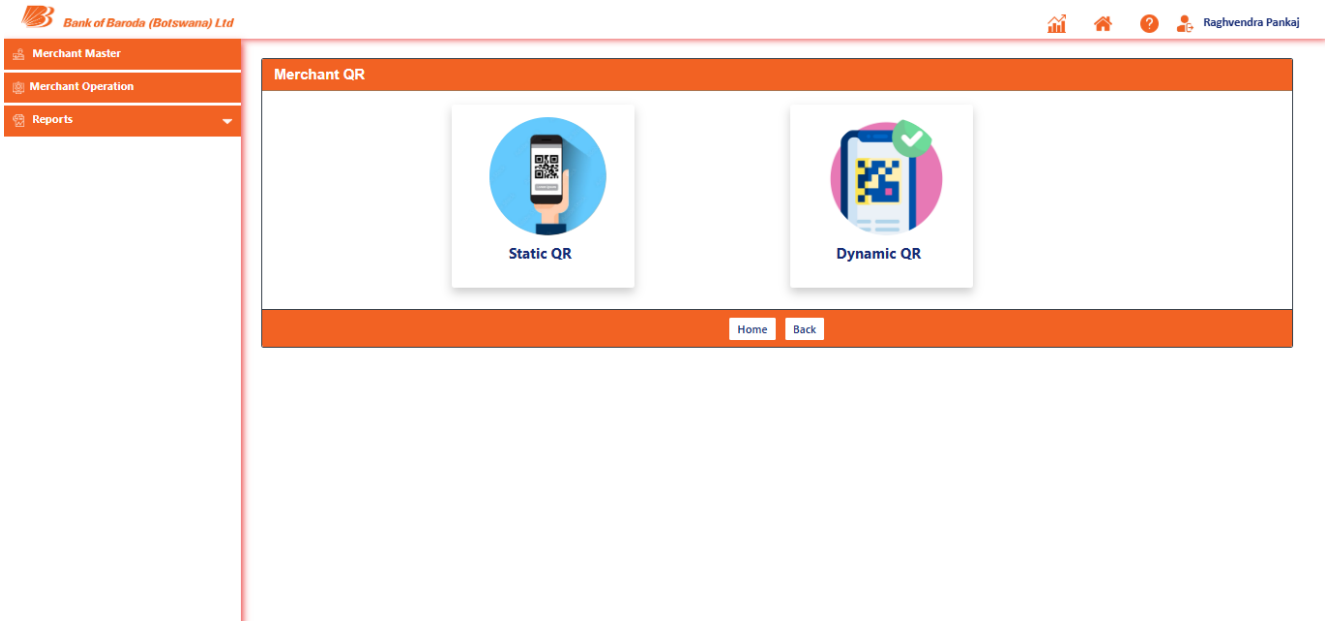
- Merchants can raise service requests to the bank if they encounter issues or need assistance.
- Service requests can be formal or informal inquiries, requests, or applications made to the bank.
- Requests can encompass a wide range of banking activities and services.



2.2.2. Merchant QR

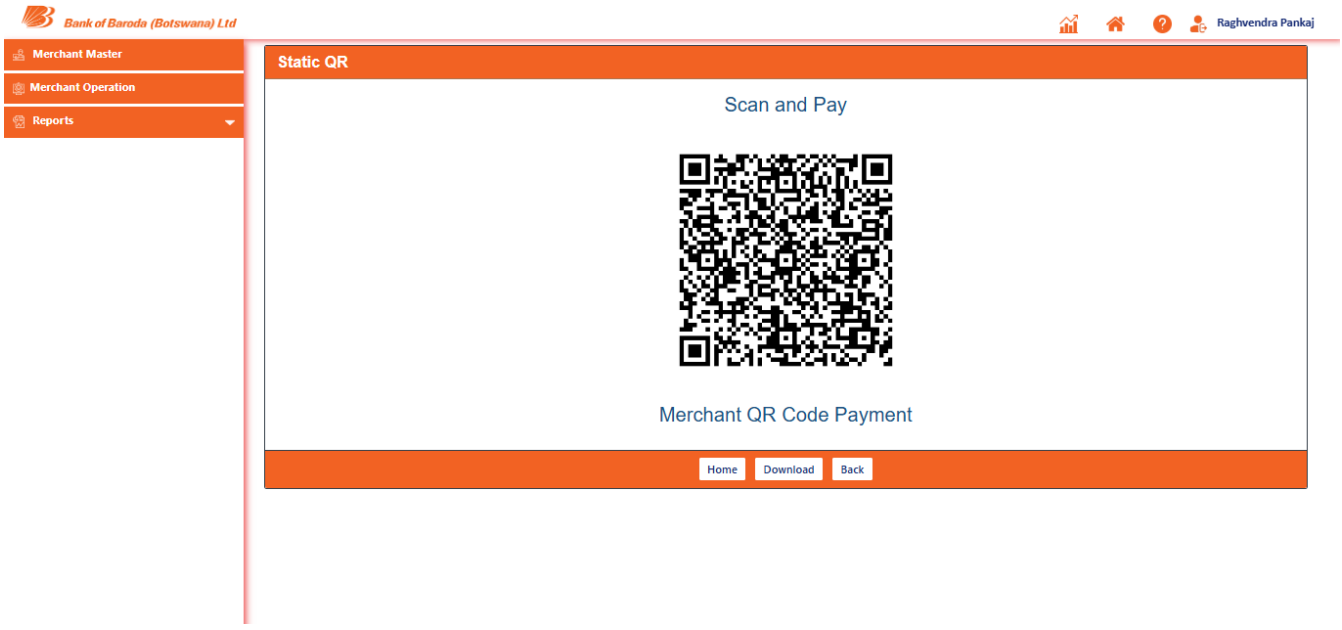
Merchants have the ability to generate two types of QR codes: static and dynamic. A static QR code is generated without an amount, while a dynamic QR code is instantly generated with an amount encoded. Merchants can share and download both types of QR codes as needed.

- Static QR
- Dynamic QR



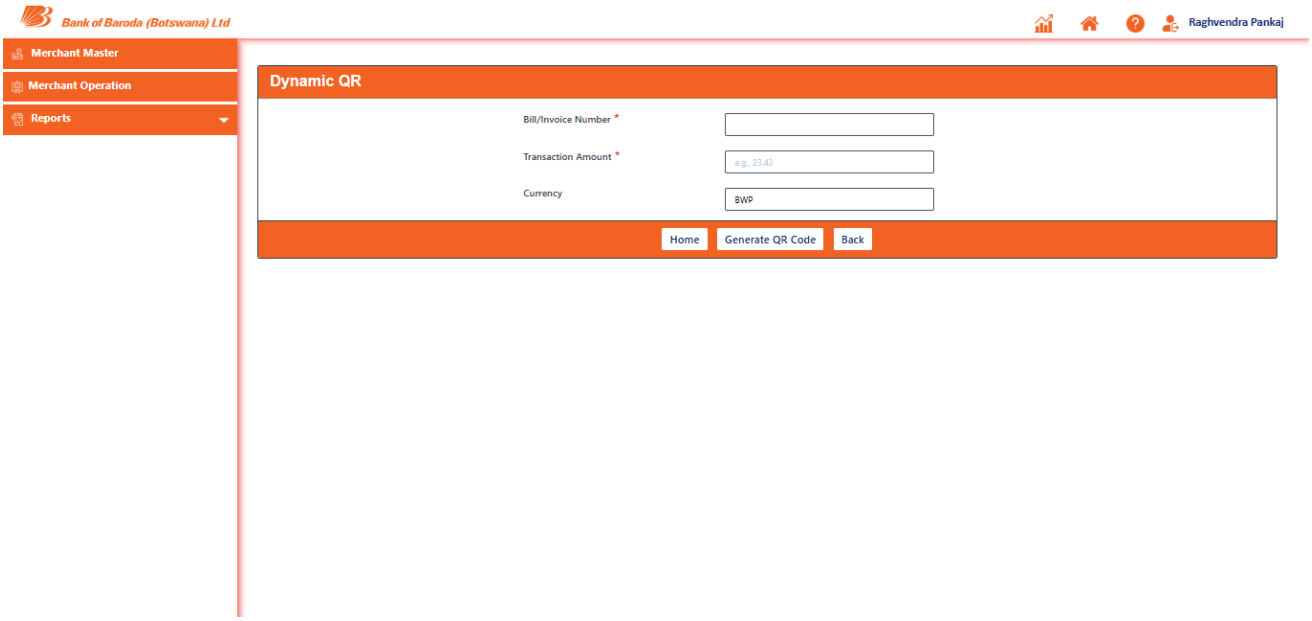
2.2.2.1. Static QR Code

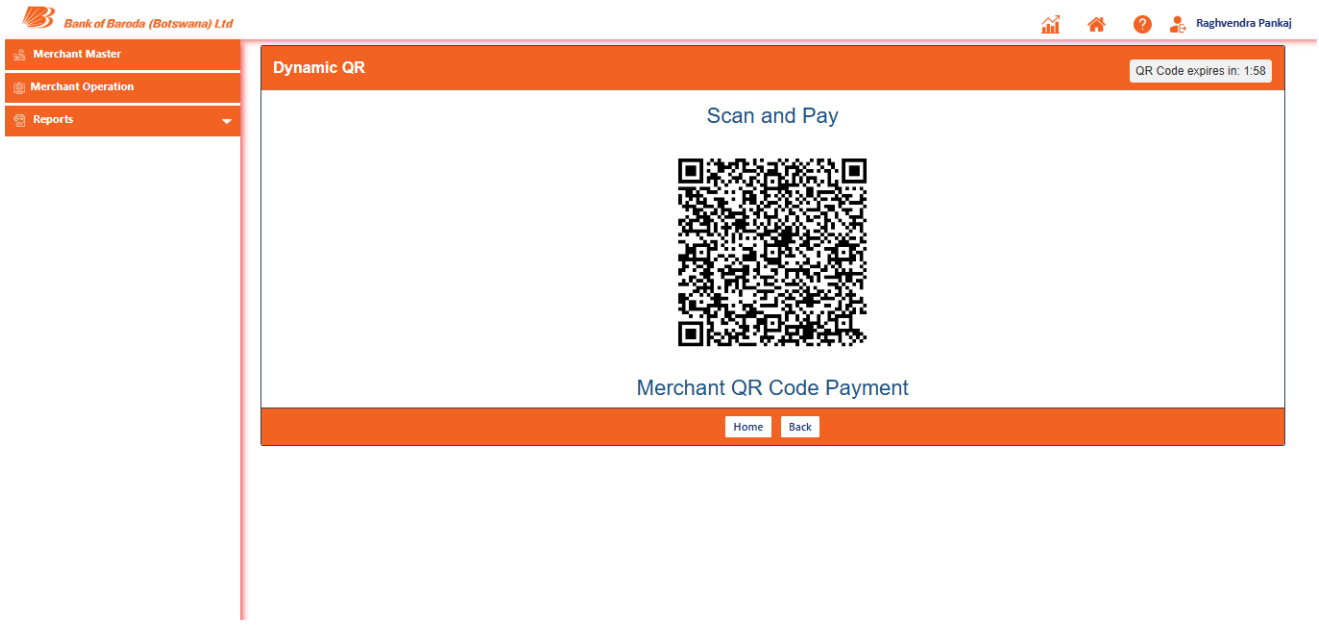
A static QR code contains fixed information, such as the merchant's name, location, and other identifying details. Customers can scan the static QR code to make payments without any additional information being transmitted



2.2.1.2. Dynamic QR Code

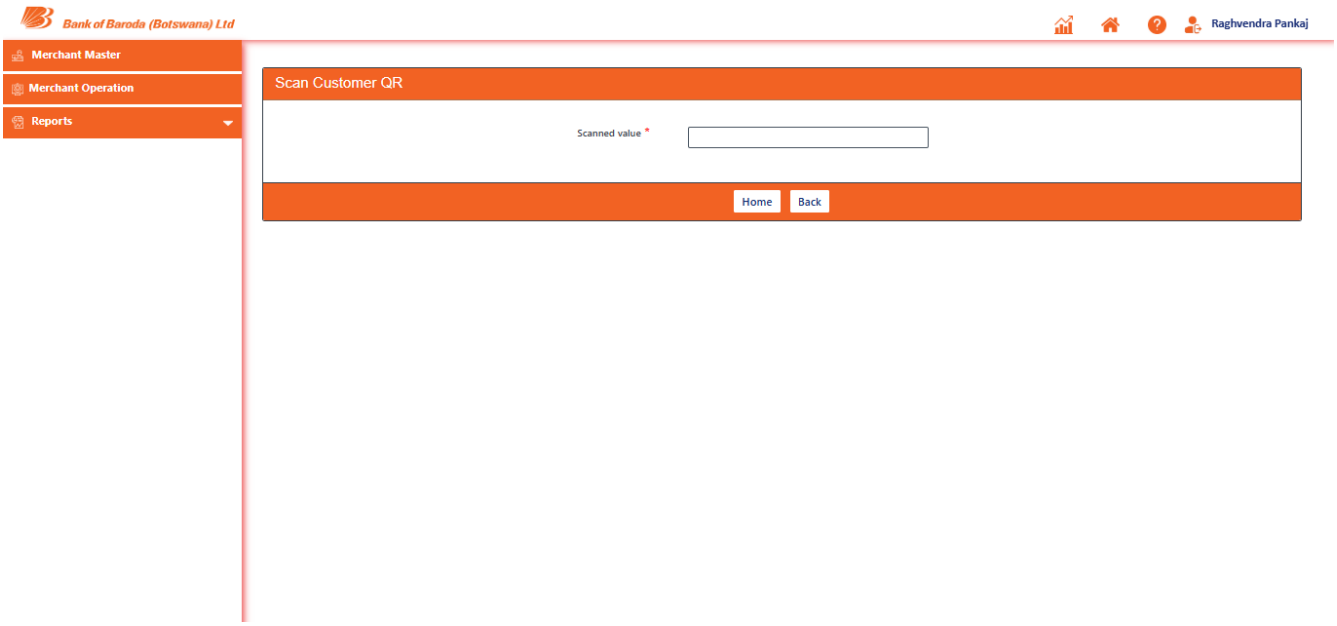
A dynamic QR code contains a URL or reference to a server-side script that generates payment information dynamically. When customers scan the dynamic QR code, their payment apps or devices interact with the server to obtain the necessary payment details

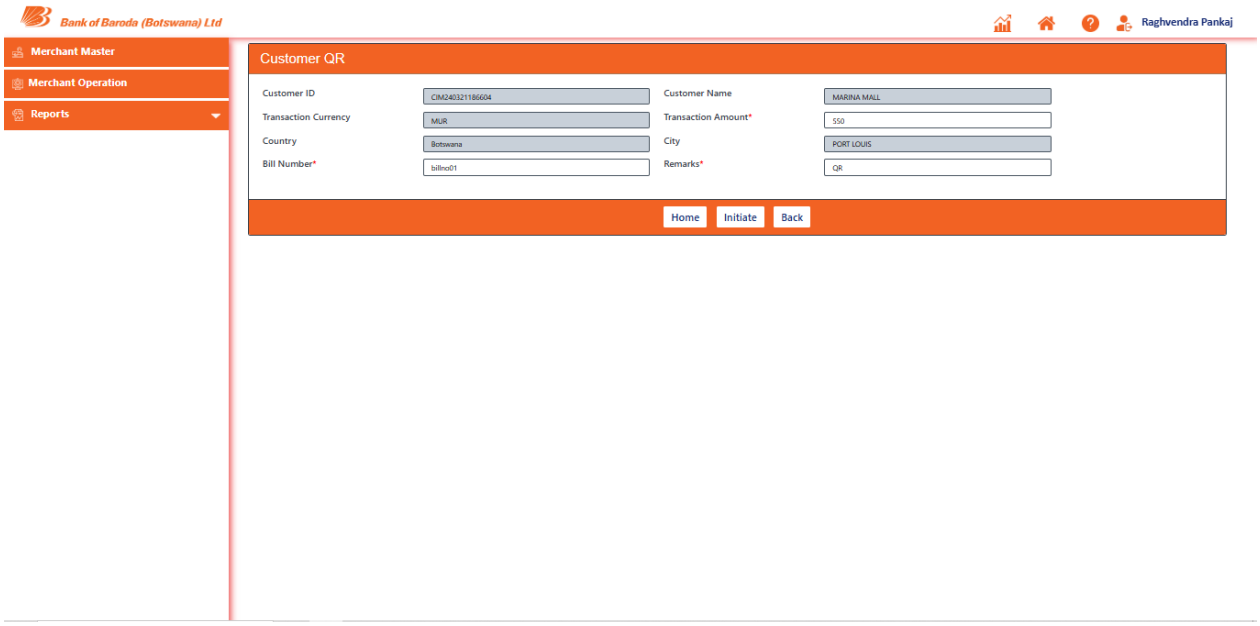


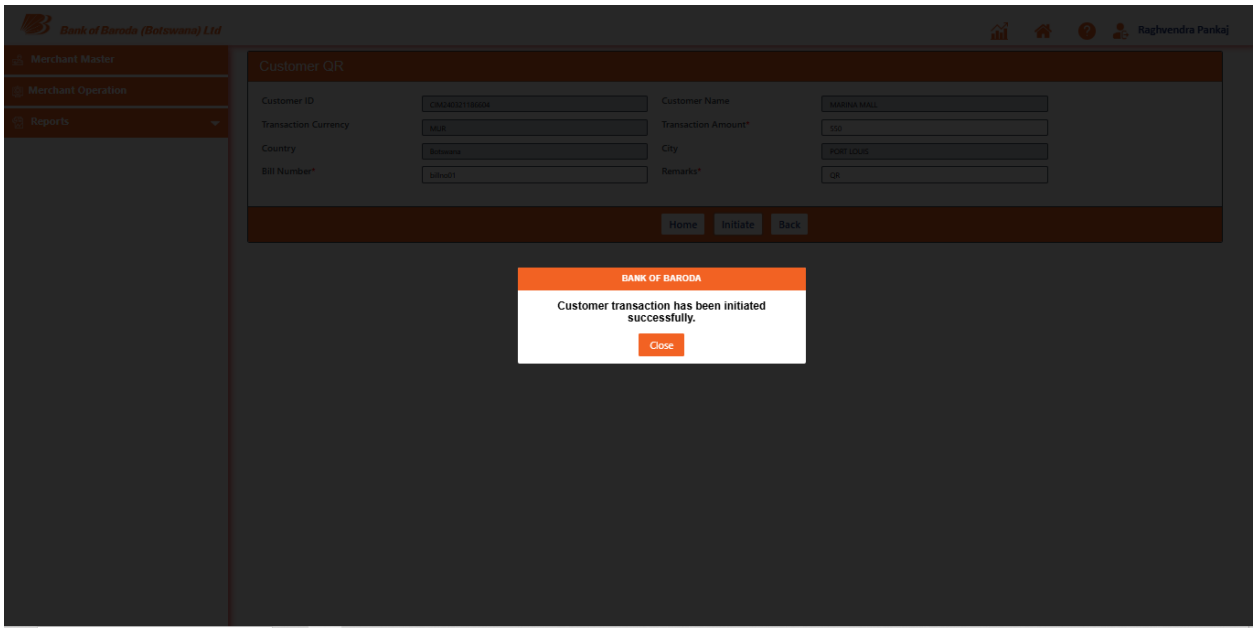


2.2.3. Customer QR

- The scanning device should be equipped with a QR code scanning app or software that can read and decode the QR code.
- Once the QR code is scanned, the merchant's scanning device extracts the payment details encoded in the QR code.
- The scanning device then sends a payment request to the payment processor or bank, along with the extracted payment details.
- The payment processor or bank processes the payment request and initiates the transfer of funds from the customer's account to the merchant's account.




Bank of Baroda (Botswana) Ltd
Raghvendra Pankaj
Merchant Master
Merchant Operation
Reports
Customer QR
Customer ID
CIM240321186604
Customer Name
MARINA MALL
Transaction Currency
MUR
Transaction Amount*
550
Country
Botswana
City
PORT LOUIS
Bill Number*
billno01
Remarks*
QR
Home
Initiate
Back

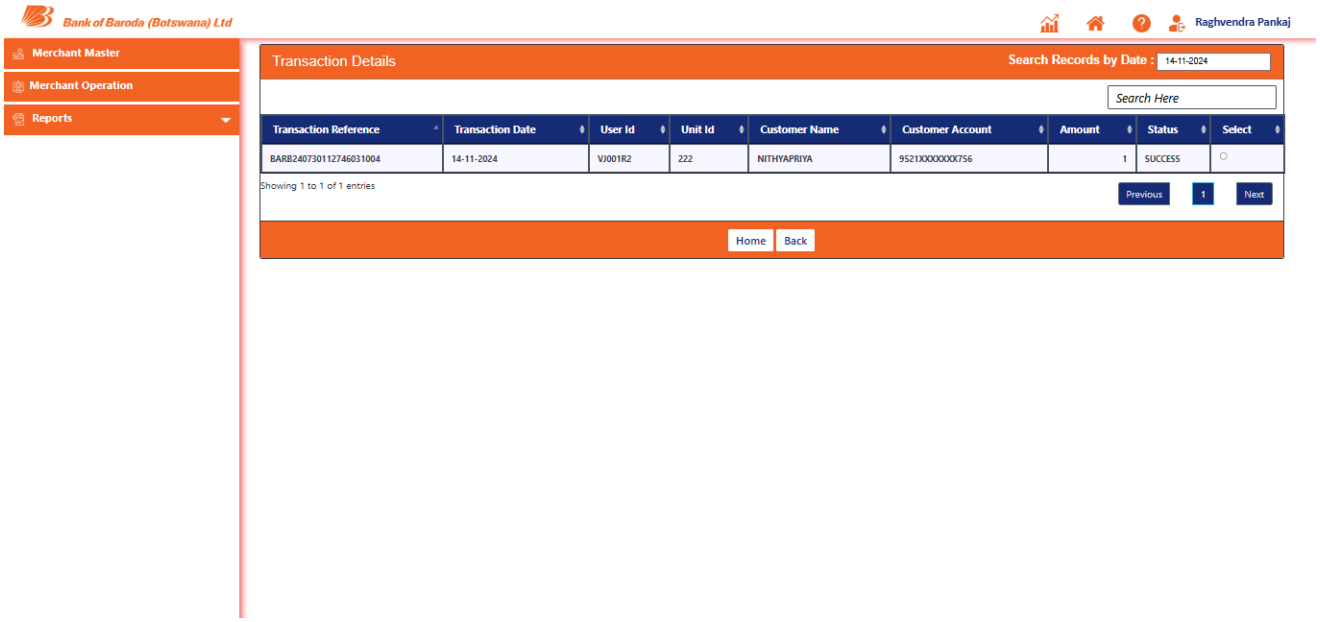

Bank of Baroda (Botswana) Ltd
Raghvendra Pankaj
Merchant Master
Merchant Operation
Reports
Customer QR
Customer ID
Customer Name
Transaction Currency
Transaction Amount*
Country
City
Bill Number*
Remarks*
Home
Initiate
Back
BANK OF BARODA
Customer transaction has been initiated successfully.
Close

2.2.4. Transaction Details

In the transaction details, merchants can exclusively view their own transactions, as opposed to the entire transaction list available in the customer transaction list.

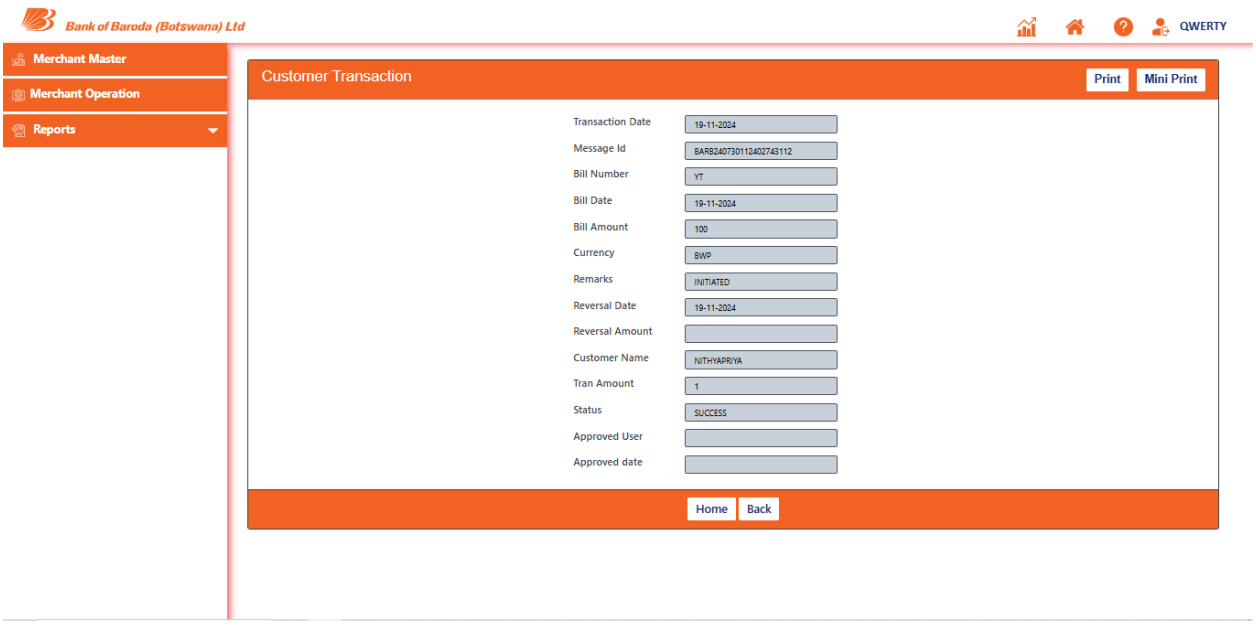
Transaction- List

Display the list of Transactions. The Screen will appear below,



Transaction- View

Display the View of Transactions. The Screen will appear below,

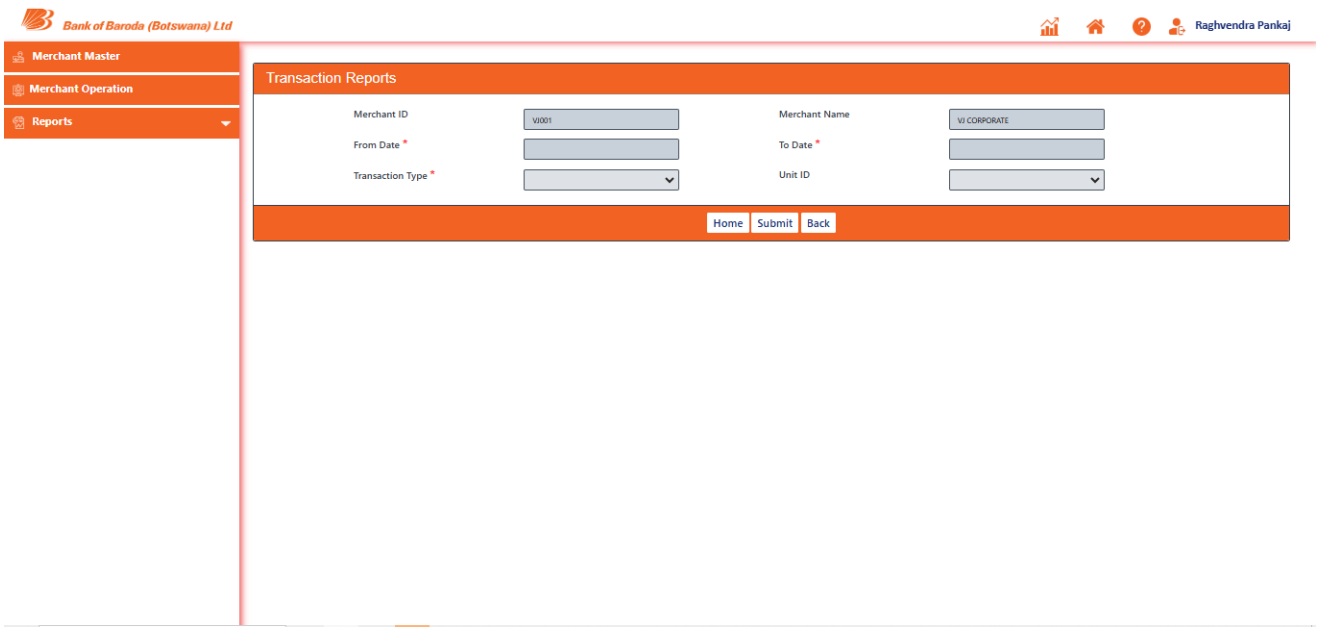


2.3. Reports

- Here We have the
    - Transaction Report
    - Charge Back Report
- For transactions, you can download them with the following options:
    - Unit Wise
    - User Wise
    - Device Wise
- You can also select a date range (from date to date).
- The available download formats are Excel and PDF.

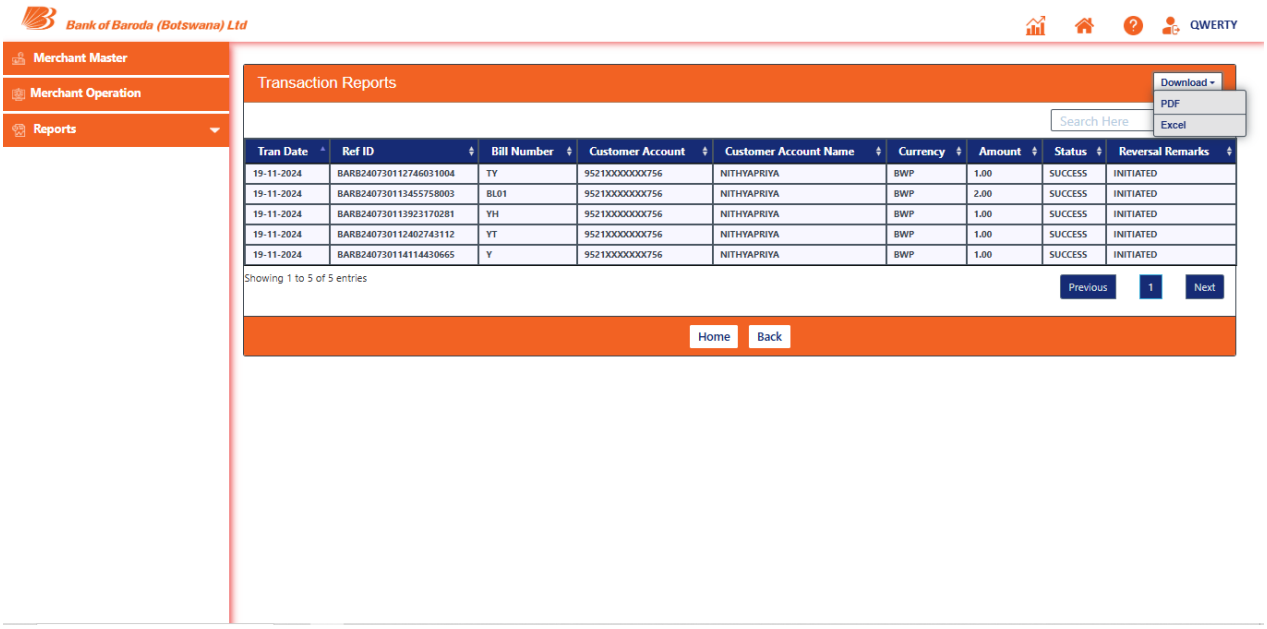
2.3.1. Transaction Report

Here, we select the transaction type and generate the report by retrieving records for the specified date.



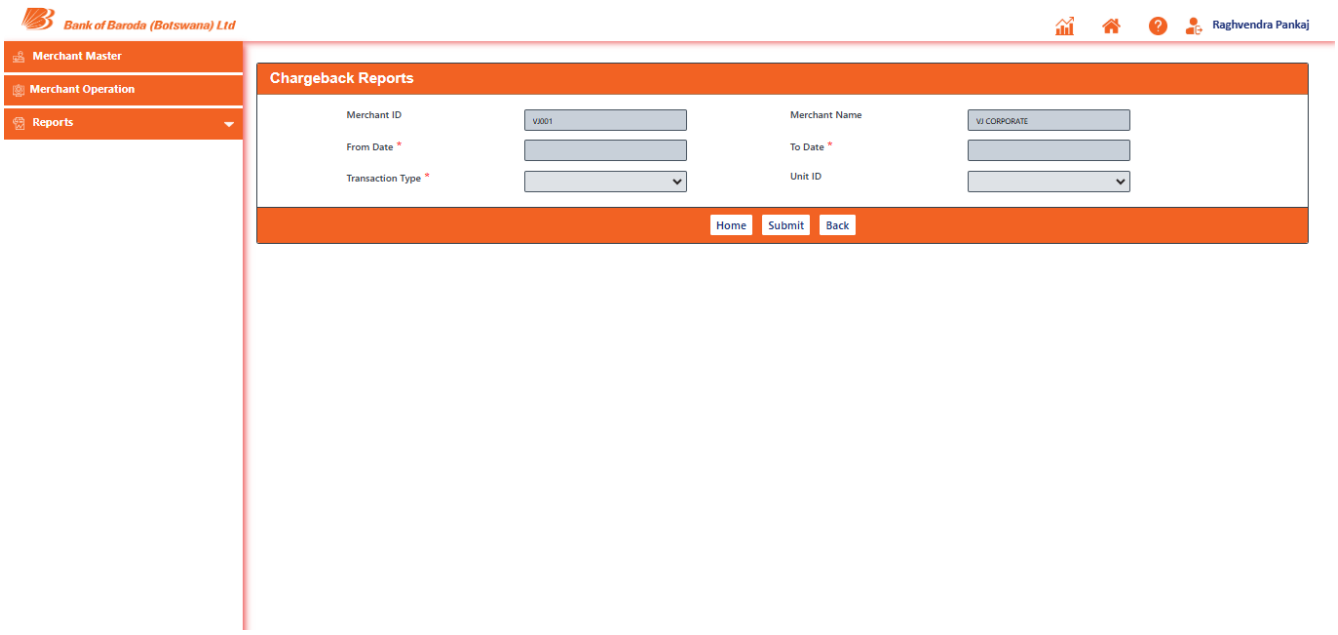
Transaction Report- List

Here, we download the transaction report by fetching the records for the desired date.



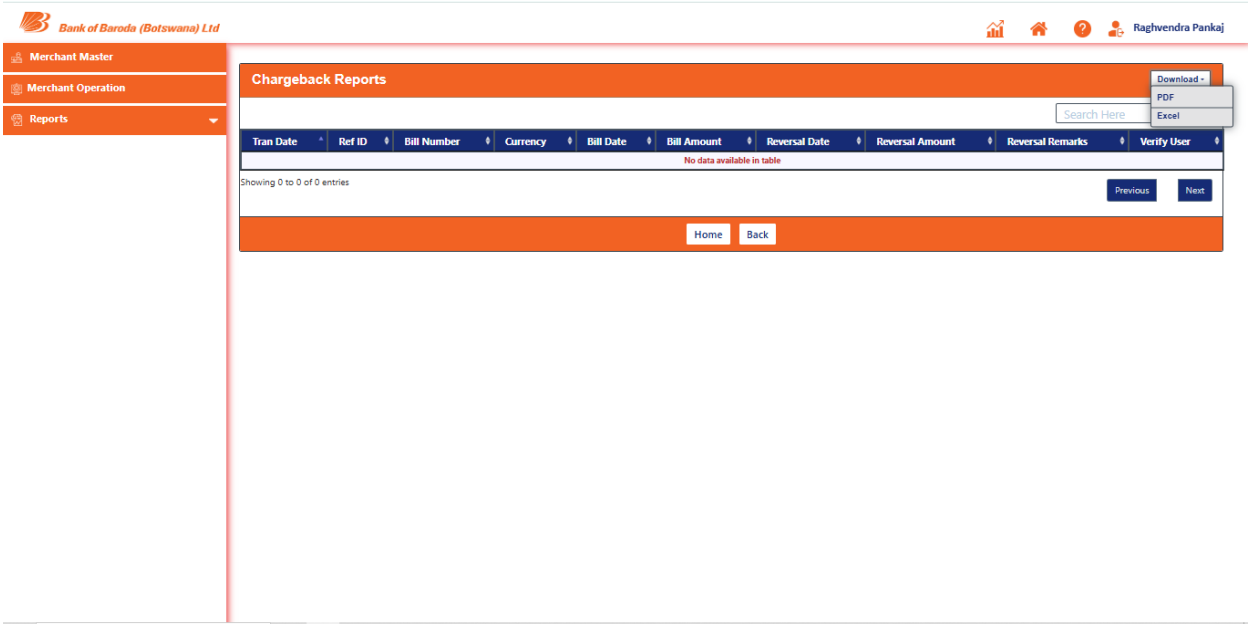
2.3.2. Charge Back Report

Here, we select the transaction type and generate the report by retrieving records for the specified date.



Charge Back Report - List

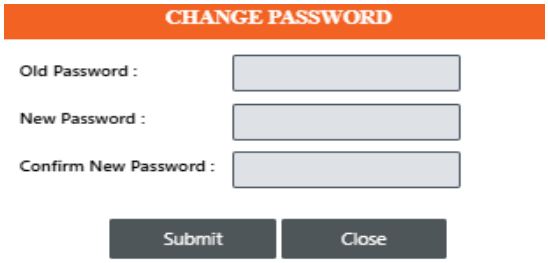
Here, we download the Charge Back report by fetching the records for the desired date.



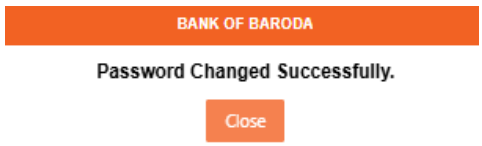
2.4. Change Password

- Users can change their existing password to a new one.
- This feature enhances account security by allowing periodic password changes.
- Ensures unauthorized access is minimized.
- After submitting the new password, a message indicating "Password changed successfully" is displayed.

Click LoginUserName in Action Panel. It displays dropdown. Then Click Change Password

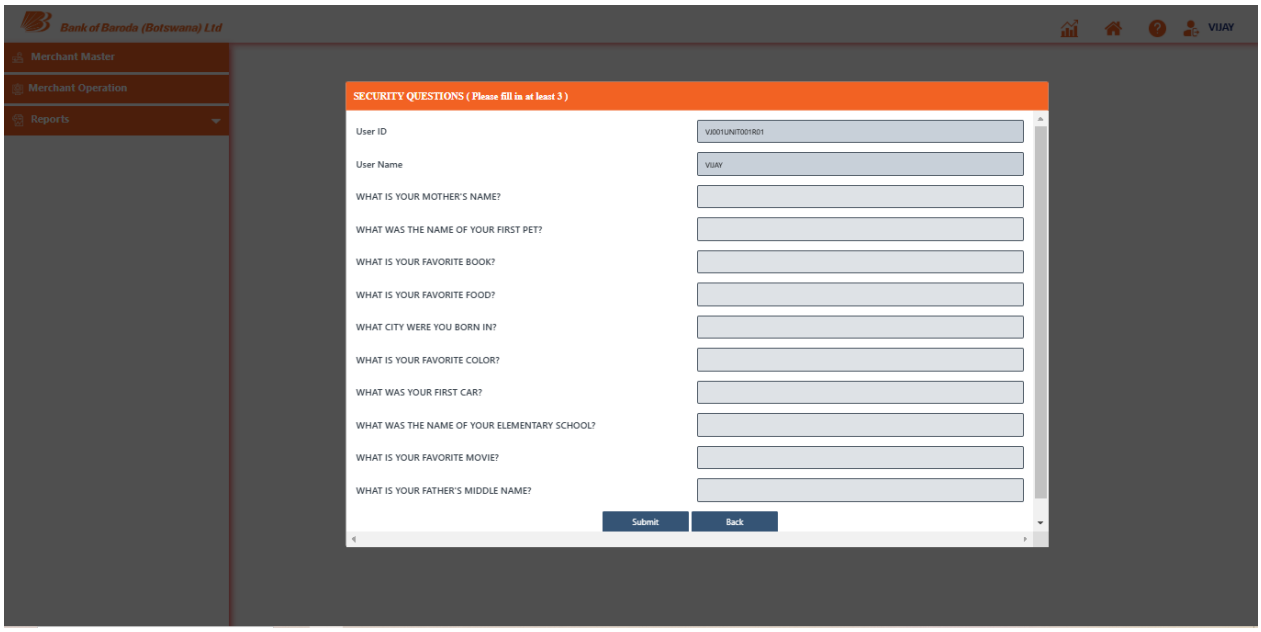


Enter the relevant data and submit.

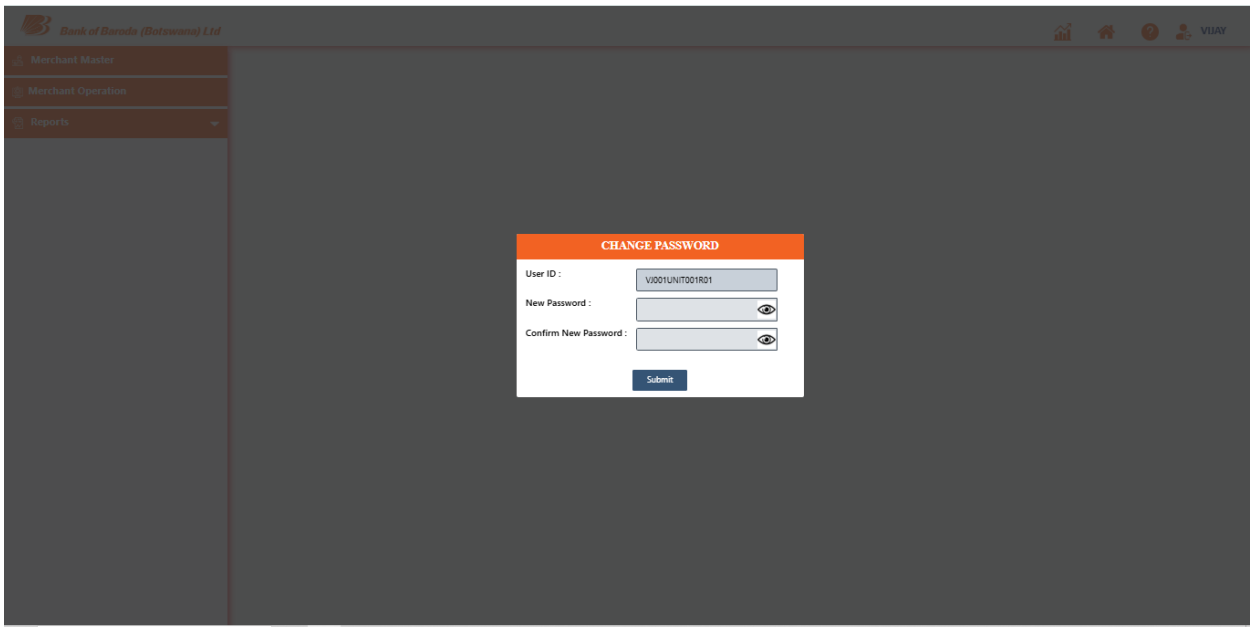


2.5 .Two Factor Authentication

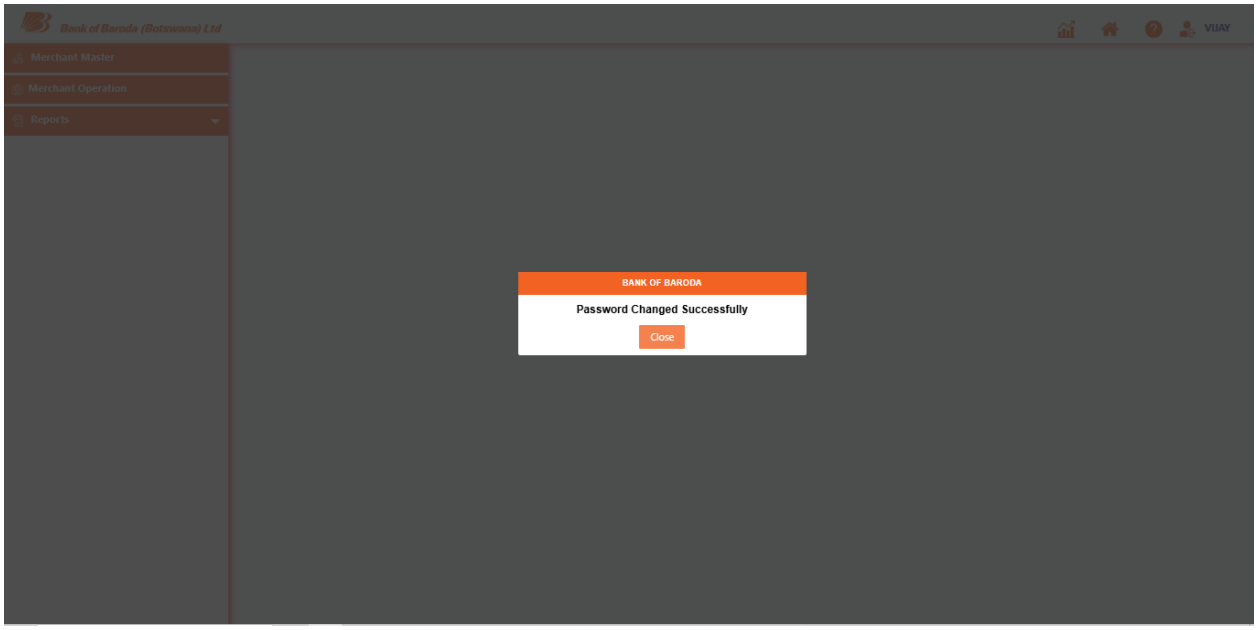
In the two-factor authentication system, new users are presented with 10 questions during their initial login , and they must provide answers to any 3 of these questions. On the "forgot password" screen, users are presented with these authentication questions. They can choose any one question to answer. After successfully answering it, they will proceed to change their password.



After answering the two-factor authentication (2FA) question, the user is redirected to the change password screen, where they are prompted to enter a new password and confirm it by re-entering the same password in a second field. Once both fields are filled and match, the user submits the form, and the system processes the change.

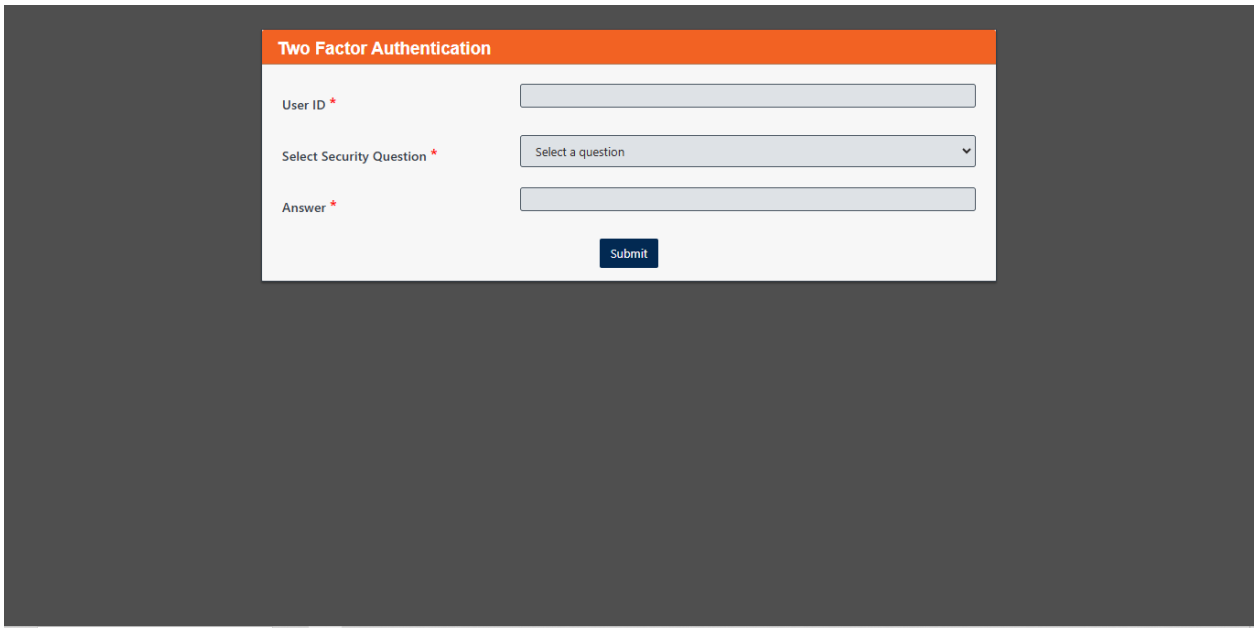


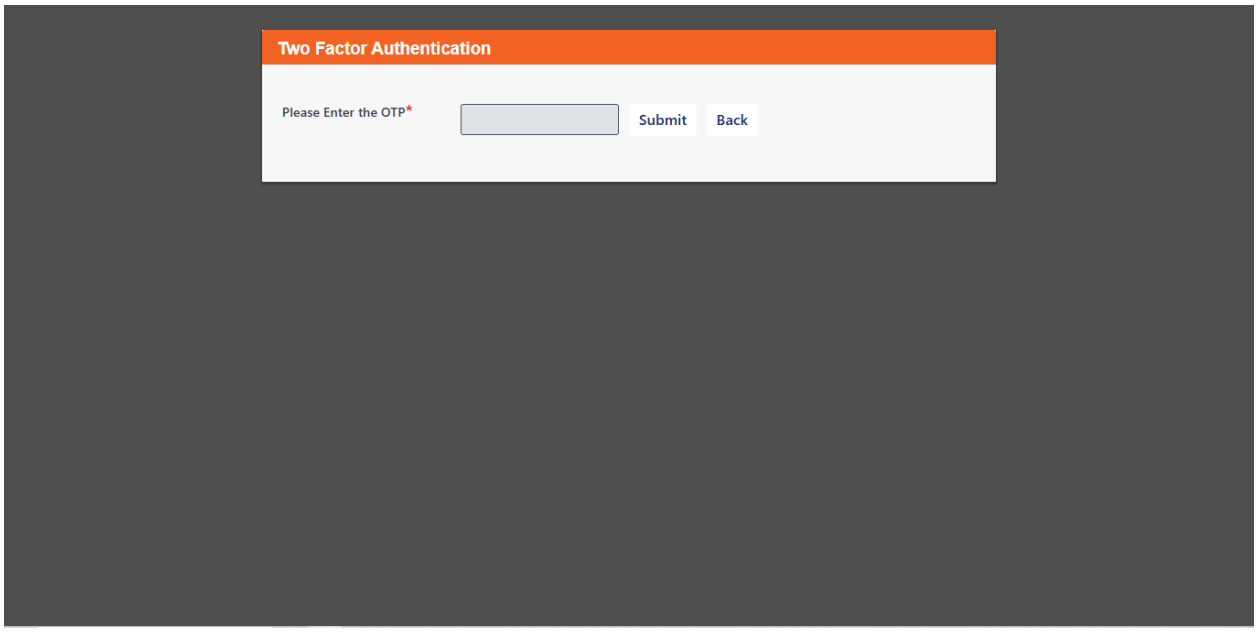
If successful, the password is updated, and the user receives a confirmation message indicating that their password has been changed successfully.



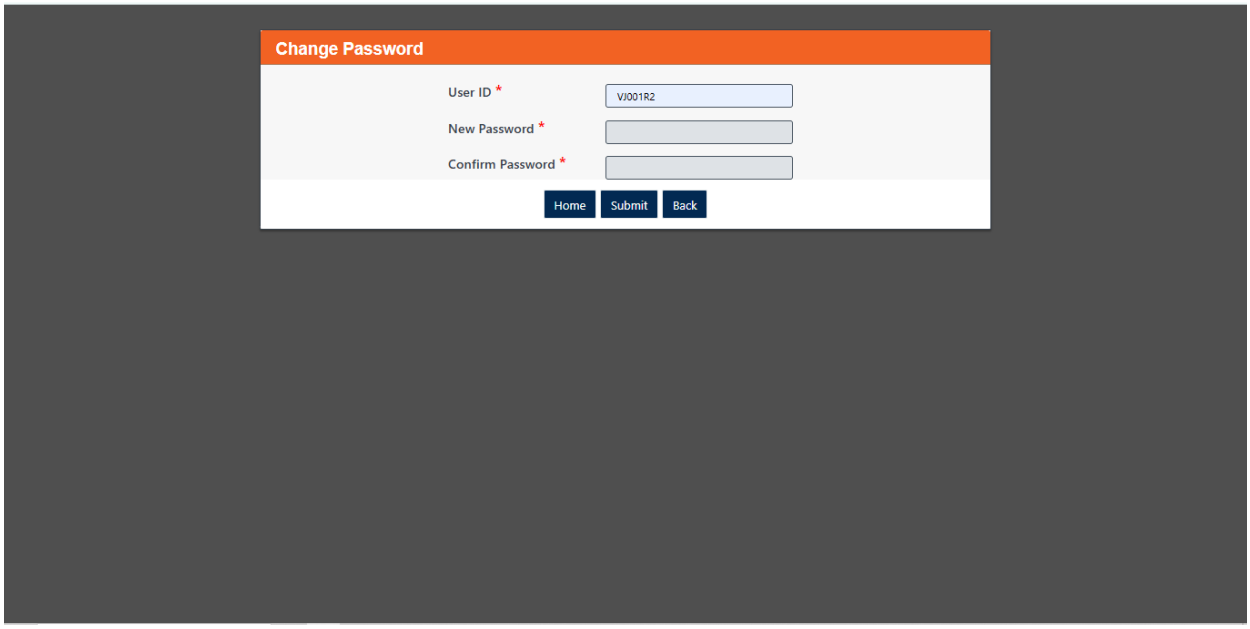
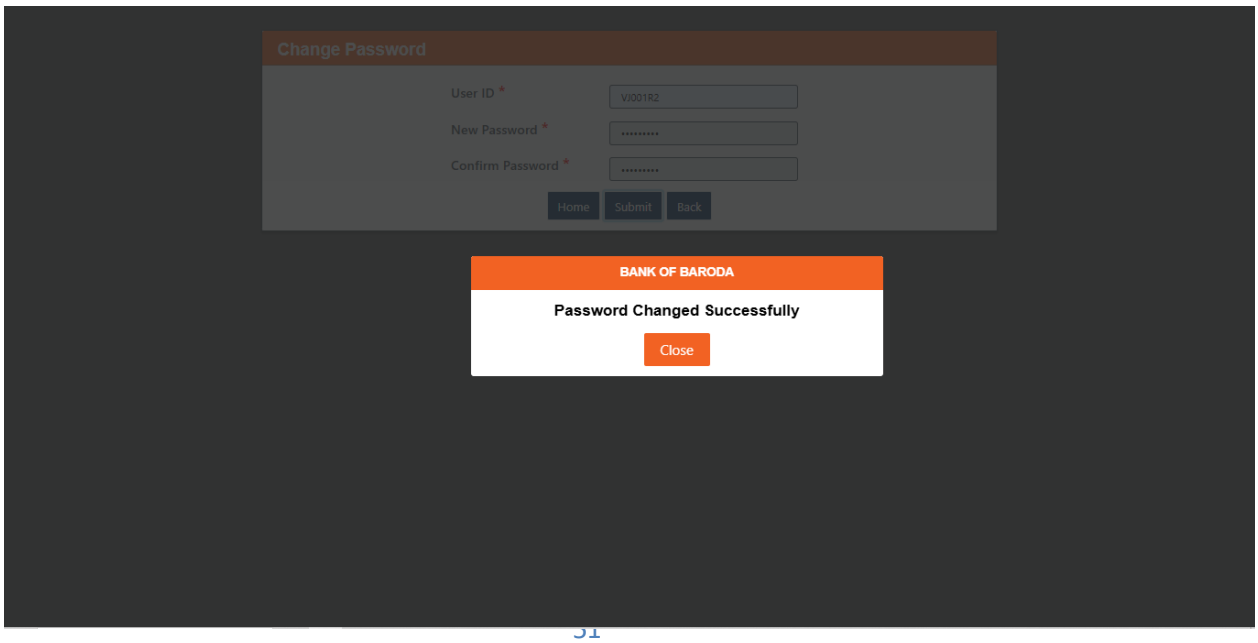
2.6. Forgot Password

In the Forgot Password Process, users are presented with that 10 authentication questions. They can choose any one question to answer. After successfully answering it, they should enter the OTP.





After the OTP is correctly entered, the user is redirected to the change password screen, where they are prompted to enter a new password and confirm it by re-entering the same password in a second field. Once both fields are filled and match, the user submits the form, and the system processes the change.



If successful, the password is updated, and the user receives a confirmation message indicating that their password has been changed successfully.