SOUTHBANK INC.

SBPAY PLATFORM:

Operating Procedures and Guidelines

Document Revision History:

Version	Date	Author	Description of Changes
1.0	06-11-2025	Norman Armian	Initial Manual/Document creation

1. INTRODUCTION

SBPay, the financial platform of SouthBank, is an innovative and versatile solution designed to bridge individuals, businesses, and government entities by enabling seamless digital financial transactions through mobile banking technology. It empowers users with a secure and efficient way to manage their finances, whether for personal banking, business operations, or public sector transactions.

Built to support a wide range of transaction types, SBPay seamlessly integrates with financial institutions, payment networks, and regulatory frameworks, ensuring interoperability and compliance with industry standards. With its user-friendly interface and security features, the platform enhances financial accessibility and promotes digital inclusion, allowing users to perform transactions such as fund transfers, bill payments, merchant transactions, and other essential banking services anytime, anywhere.

This manual serves as a comprehensive guide to SBPay's features, functionalities, operational processes, and compliance requirements. It is designed to equip users, stakeholders, and financial partners with the knowledge needed to navigate the platform effectively, optimize its capabilities, and ensure adherence to financial regulations and best practices.

2. PURPOSE

The SBPay Manual of Operations, General Guidelines, and Procedures establishes a comprehensive framework for the secure, consistent, and efficient management of SBPay's financial platform. It serves as the primary reference for all users, stakeholders, and operational teams, ensuring standardized practices for platform usage, transaction processing, and system administration.

This manual defines essential policies, procedures, and operational standards to maintain full compliance with regulatory requirements and applicable financial regulations. It also incorporates security protocols, risk management strategies, and governance measures to safeguard financial transactions and protect user data.

In addition, the manual provides clear guidelines on user roles and responsibilities, customer support escalation, fraud prevention, and system maintenance. Its purpose is to enhance operational efficiency, reduce risk exposure, and promote best practices in managing digital financial services.

By adhering to the principles set forth in this manual, SBPay ensures seamless integration with financial institutions, fosters transparency, and strengthens user trust, reflecting its commitment to delivering a secure, reliable, and innovative financial ecosystem

3.   **DEFINITION OF TERMS – SBPAY SERVICES, OPERATIONS, AND DOCUMENTATION**

TERM	DEFINITION
SBPay	The bank's proprietary digital financial platform offering secure mobile and web-based services such as fund transfers, bills payment, account management, and corporate disbursements.
SBPay Portal	A web-based interface used by internal personnel and corporate users to perform administrative tasks, monitor transactions, and manage accounts.
SBPay Mobile App	The mobile application version of SBPay that allows individual users to access digital financial services, including money transfers, bills payment, and balance inquiries.
EPFS (Electronic Payment and Financial Services)	A suite of digital financial services offered through SBPay in compliance with BSP regulations, enabling users to conduct cashless transactions.
Fund Transfer – P2P (Person-to-Person)	A feature allowing users to send money directly to another SBPay user within the platform.
Interbank Transfer	The ability to transfer funds from an SBPay-linked account to other banks using PESONet or InstaPay facilities.
Bills Payment	A service that enables users to pay for utilities, government fees, and merchant obligations through the SBPay platform.
Buy Load / Mobile Top-Up	A prepaid service allowing users to purchase mobile credits for themselves or others using SBPay.
Scan to Pay (QR Payments)	A digital payment feature that allows users to pay participating merchants by scanning QR codes through the SBPay app.
Request Money	A function that enables users to initiate a payment request from another user, who may approve and fulfill the transfer.
Transaction Limit	The maximum amount that can be transacted per operation or within a specific period, based on the user's profile or account tier.
Wallet Limit	The cap on the total amount a user can hold in their SBPay digital wallet, subject to regulatory and internal policies.
User Tiering	The classification of users (e.g., Basic, Verified, Premium, Corporate) based on KYC level and transactional behavior.
Transaction History	A chronological record of user activities and completed transactions within the SBPay system.
Cut-off Time	The specified time each day after which transactions are processed on the next banking day (applicable to services like PESONet).

TERM	DEFINITION
Transaction Queue	A pending state where transactions await validation, system checks, or external clearing before final posting.
Transaction Reversal	The corrective process to cancel, refund, or adjust a completed transaction due to error or dispute.
Account Linking	The connection of a user's SBPay profile to their current or savings account (CASA) to enable fund movement.
CASA (Current Account / Savings Account)	A deposit account associated with SBPay that enables financial transactions.
CIF (Customer Information File)	A database of client details used for verification, compliance, and service delivery purposes.
KYC (Know Your Customer)	The mandatory process of verifying a user's identity and assessing risk to comply with AML and financial regulations.
AML (Anti-Money Laundering)	A legal and procedural framework aimed at detecting and preventing the use of SBPay for illicit financial activities.
User Authentication	The process of validating user credentials (e.g., username, password, and OTP) for secure access to the SBPay platform.
OTP (One-Time Password)	A temporary, system-generated code used to verify a user's identity during login or transactions.
Onboarding	The registration and activation process for new users or partners, including identity verification and system enrollment.
Information Security	A set of protocols and controls protecting data integrity, confidentiality, and system availability within SBPay.
Disaster Recovery (DR)	An emergency plan and set of systems to restore SBPay services following outages, breaches, or disruptions.
Business Continuity Plan (BCP)	A strategic framework ensuring uninterrupted access to SBPay services during adverse events or disasters.
Service Downtime	Periods when SBPay services are temporarily unavailable due to maintenance or system failure.
Service Availability Window	The period during which SBPay services are expected to be fully functional and accessible to users.
System Admin	An authorized user with the highest level of control over SBPay, responsible for managing settings, users, and security.
Retail User	An individual user who accesses SBPay services via mobile or online platforms for personal financial needs.

TERM	DEFINITION
Corporate User	A business client using SBPay for bulk transactions such as payroll, supplier payments, and collection services.
User Roles	Defined access levels within the SBPay system (e.g., Admin, Branch Ops, Corporate User) according to functional responsibilities.
Support Escalation	The structured approach for resolving technical or service-related issues that require multiple levels of response.
Customer Support Ticket	A logged record of an incident or inquiry submitted by users to be tracked and addressed by the SBPay support team.
Compliance Check	A review mechanism, either manual or automated, to ensure all SBPay operations adhere to regulatory and internal policies.
Audit Trail	A system-generated log of user activities and changes made to SBPay, used for monitoring, accountability, and regulatory compliance.
Sandbox Environment	A testing environment where developers and partners can simulate SBPay features without impacting live systems.
Regulators	Government authorities such as the BSP (Bangko Sentral ng Pilipinas), AMLC, and NPC, which oversee SBPay's compliance with financial, anti-money laundering, and data privacy regulations.
Data Privacy	Adherence to the Data Privacy Act of 2012, ensuring responsible collection, storage, and processing of user information within SBPay.
SMS Notification	Automated messages sent by SBPay to users for transaction alerts, security updates, and service announcements.
Service Monitoring Dashboard	An internal tool used by administrators to monitor real-time service status, usage metrics, and system health across SBPay platforms.
Whitelisting	A security mechanism where only approved IP addresses or mobile numbers are allowed to access or interact with specific SBPay features.

4. MOBILE BANKING APPLICATION

Sections: 4.1 - 4.9

SBPay is a mobile banking solution designed to serve individual customers conveniently through their mobile phones. The application is available for download and installation on both Android and iOS platforms.

Access to SBPay requires authorized user credentials, which are uniquely assigned upon successful registration and activation. The onboarding process includes a standard Know Your Customer (KYC) procedure conducted at the branch level by designated personnel.

Upon completion of the KYC process, the client will receive system-generated credentials, including a temporary username and a token valid within 3 days. These credentials will be required for completing the activation process and gaining full access to the mobile banking application.

4.1 KNOW YOUR CUSTOMER (KYC) PROCESS IN SBPAY

The KYC (Know Your Customer) process in SBPay is a critical component of the bank's compliance with Anti-Money Laundering (AML) regulations. It ensures the verification of clients' identities, helping to prevent illegal activities such as money laundering, terrorist financing, and fraud. By verifying the true identity of customers, the bank upholds trust, security, and compliance.

To open an SBPay account, clients must complete the KYC process by providing the following mandatory information:

1. **Photograph**
   - A live image or a recent 2x2 picture
2. **Identification Documents**
   - A clear copy of both the front and back of a government-issued ID
3. **Personal Information**
   - First name
   - Middle name
   - Last name
   - Suffix (if applicable)
4. **Address Details**
   - Both current and permanent addresses, formatted as:
     - Region/Province/City/Barangay/ZipCode/Unit#/Subdivision/Street/House#
5. **Civil Status**
6. **Nationality**
7. **Mother's Maiden Name**
8. **Contact Information**

- Mobile number

9. **ID Details**
   - Type of ID
   - ID number
   - Expiry date (if applicable)
   - Remarks on ID validity (if necessary)

4.2 KYC Client Assessment

As part of the KYC process, clients are rated based on the evaluation conducted by the presiding branch personnel in accordance with the bank's KYC protocols. This rating categorizes clients into three classifications:

- **High Risk**
- **Medium Risk**
- **Low Risk**

This module includes the capability to capture and securely store both the client's photograph and images of their provided identification document (front and back).

Birthdate 📅 * *(format: mm/dd/yyyy)*
10/04/1969

Place of Birth *
Dangcagan Bukidnon

Gender * ○ Male ● Female

Mother's Maiden Name
Leonor Relos Pagal

Contact No. *
09068719495

Nationality *
FILIPINO

Civil Status *
Married

Nature of Work
Teaching

Job Title
Teacher

ID. Type *
GSIS

ID No. *
006-003-0237-6

Expiry Date

ID Remarks
UMID ID

This module captures additional details about the client that go beyond the basic KYC requirements. It ensures a comprehensive profile by collecting supplemental information, which may include Place of birth, Mother's maiden name, or other relevant data necessary for a more in-depth understanding of the client's personal and financial background.

Risk Rating*
Select Risk Rating

Upload E-SIGNATURE

FOR BANK'S USE ONLY

AMLC
Choose File No file chosen

This module allows branch personnel to assess and assign a risk rating to the client based on the evaluation conducted during the KYC process. The risk rating—categorized as High, Medium, or Low—helps the bank implement appropriate monitoring and

compliance measures tailored to the client's profile. The result also from AMLC checker adds up to the validation of the client's risk exposure.

```
MEMBERSHIP
                                                              ☑ Edit

Main Branches          Initiator Branches       Membership Status
SBI-KITAOTAO           SBI-KITAOTAO             Active
```

This module designates the servicing branch for the client, ensuring that the account is tagged and registered under a specific branch. This linkage facilitates streamlined account management and provides a clear point of service for the client.

OPERATIONAL GUIDELINE (Sections: 4.1 – 4.2):

To ensure a seamless end-to-end process, new accounts personnel or designated staff must verify that clients meet all requirements before initiating the actual KYC procedure. The following steps outline the necessary activities:

1. **Pre-assessment:**

Prior to beginning the KYC process, a pre-assessment should be conducted. This involves confirming that the client is physically present at the branch and able to provide a valid identification document containing a photo and other essential details.

2. **Handling Missing or Questionable Documentation:**

If a client is unable to provide the required documents then no account shall be created, or if any documentation appears questionable, the bank's Anti-Money Laundering (AMLC) procedures must be followed. For detailed steps, refer to Attachment: _____ [AMLC Policy].

3. **ID Expiry:**

For identification documents with an expiration date, the expiry must be recorded. This ensures that the KYC remains updated with valid information.

4. **KYC Form Completion:**

Clients are required to fill out a KYC form with all necessary details before account registration or application processing.

5. **Contact Information:**

It is essential to collect the client's contact number and email address, as these will be used for important notifications and account activation.

6. **Incomplete Requirements:**

In cases where clients cannot provide complete documentation, branch personnel have the option to save the application as a draft. However, records saved as drafts will not grant the client access to the account or any of its services until all requirements are fulfilled.

7. **Draft Record Accessibility:**

Draft records are saved in the KYC module and can be retrieved for future use once the client submits the necessary documents.

4.3 Account Activation (Token and Username)

Upon successful completion of the KYC process, the client will receive an SMS notification containing a temporary username and a token required for account activation.

To activate the newly created account, the client must follow these steps:

1. **Download the Mobile Application**
    - Access the app through **Google Play Store** (for Android users) or **App Store** (for iOS users).

2. **Install and Launch the Application**
    - Complete the app installation and open it on the mobile device.

3. **Verify Access**
    - Select the **Verify Access** menu within the app.
    - Input the temporary username and token received via SMS.

4. **Create Permanent Credentials**
    - Define a personal username and set a secure password.
    - Confirm the entries to finalize the activation process.

5. **Activation Confirmation**
   - Upon successful completion, the system will display a congratulatory notification, indicating that the account has been activated and is ready for use.
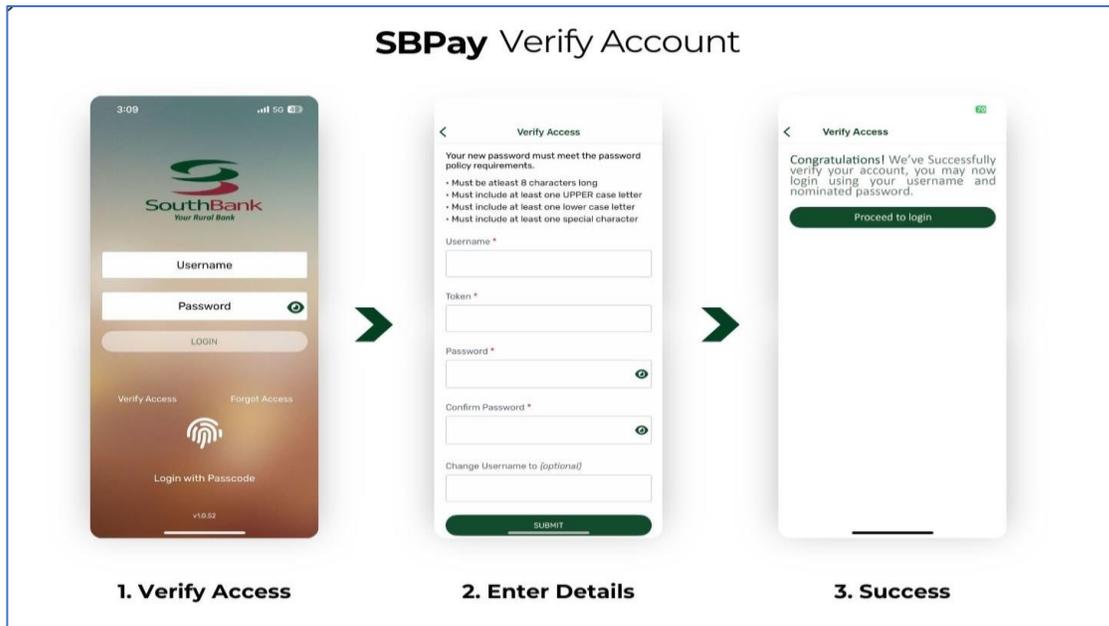
This process ensures a secure and seamless activation experience for clients, granting them immediate access to their SBPay accounts. Additionally, it allows clients to nominate their desired username. The system enforces a standard minimum password requirement of 8 characters, including a combination of alphanumeric and special characters. If the password does not meet these criteria, an error notification will prompt the client to make the necessary adjustments.

MOBILE APP TRANSACTIONS

4.4 P2P SEND MONEY VIA ACCOUNT NUMBER: QUICK AND EASY FUNDS TRANSFER

The Peer-to-Peer (P2P) "Send Money" feature in the SBPay Mobile App provides a seamless way to transfer funds between SBPay accounts. Follow these simple steps to complete a transaction:

1. **Login to Your Account**
   - Open the SBPay Mobile App and log in using your credentials.

2. **Access the "Send Money" Feature**
   - Tap the **Send Money** menu option from the app's dashboard.

3. **Initiate the Transfer**
   - On the "Send Money" menu, click **Transfer**.
   - Enter the **destination account number** and the **amount** you wish to transfer.

SBPay Send Money (P2P)

1. Send Money   2. Transfer   3. Account Number

www.southbankinc.com
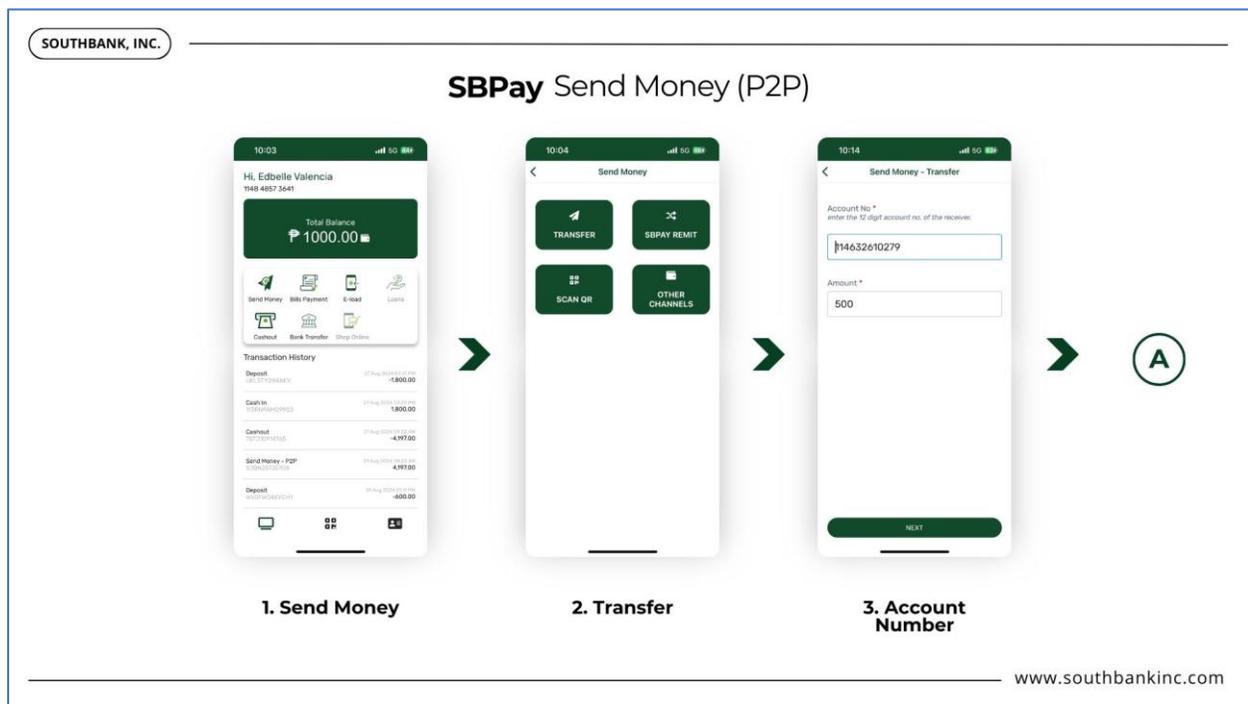
4. **Review Transaction Details**
   - A confirmation page will appear, displaying:
     - Recipient account information
     - Amount to be sent
     - Applicable fees
     - Total amount (including fees)
   - Carefully review all details.

5. **Complete the Transfer and OTP confirmation**
   - Tap the **Send Now** button to finalize the transaction.
   - The system shall push a **one-time PIN (OTP)** to confirm and proceed on the transaction.

6. **Transaction Summary**
   - After processing, a summary page will display:
     - Transaction details
     - Confirmation of the successful transfer
   - Options available:
     - **Download Image** of the transaction for your records
     - **Close** the transaction
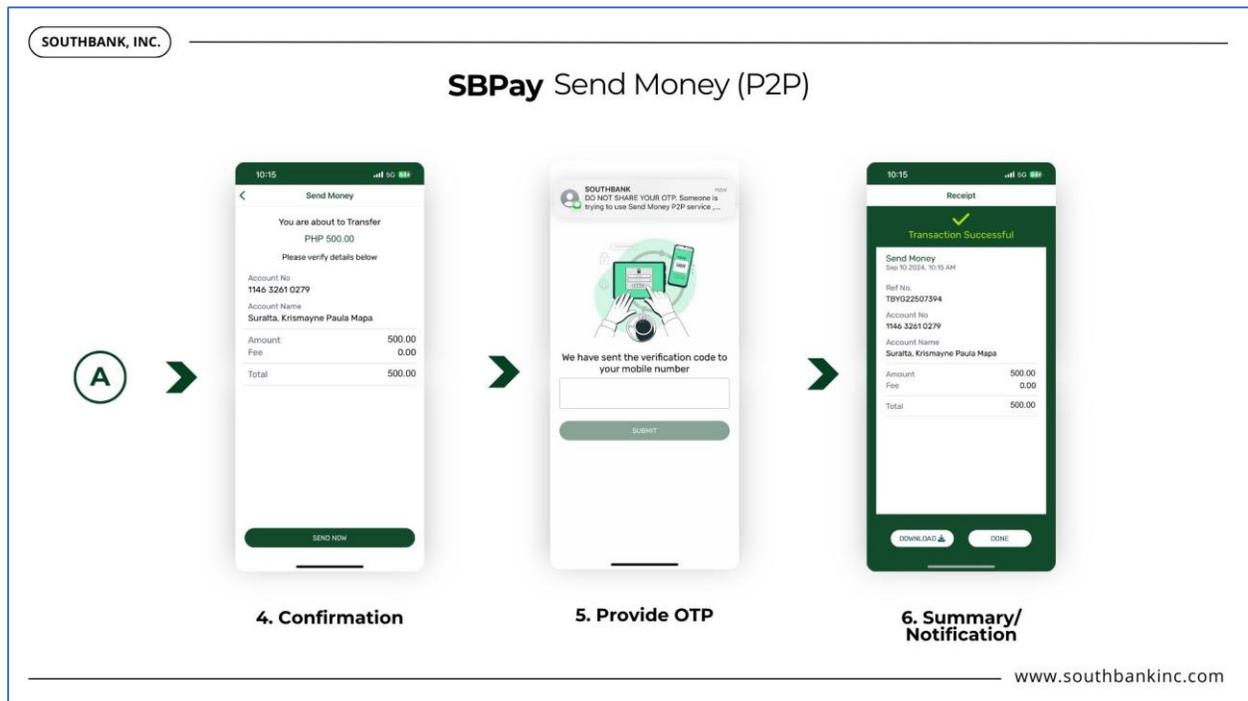
This intuitive process ensures a secure, efficient, and user-friendly experience for transferring funds through SBPay.

OPERATIONAL GUIDELINES (SECTION 4.4):

To ensure seamless fund transfers using the SBPay mobile app, users must adhere to the following standard guidelines:

1. Login Verification
- Securely log in to the SBPay mobile banking app using your unique credentials (username and password, PIN code, or biometric login).
- This step ensures that only authorized users can initiate transactions.

2. Internet Connectivity and Fund Availability
- Ensure a stable internet connection throughout the transaction to prevent interruptions.
- Verify sufficient funds in your account before initiating the transaction.
- The system will automatically check your account balance to confirm fund availability.

3. Insufficient Funds Handling
- If your account has insufficient funds to cover the transaction, the system will halt the process.
- A notification will alert you of the issue, allowing you to address the balance before proceeding.

4. Accuracy of Recipient Account Number
- Enter the recipient's account number accurately to avoid sending funds to the wrong account.
- The system will validate the entered account details before processing the transfer. If incorrect, you will be prompted to correct them.
- In the event of mistakenly transferring funds to an incorrect account:
    a) File a dispute through the **Dispute Resolution and Reconciliation Procedure** for a manual reversal.
    b) Follow the detailed steps outlined in the procedure to resolve such cases.

5. Transaction Processing
- After verification, the sender's account balance will be debited by the transfer amount, including applicable fees.
- The receiver's account will be credited in real time, confirming a successful transfer.
- Notifications will be provided to both parties to confirm transaction completion.

4.5 SEND MONEY VIA QRCODE:

The **Send Money via QR Code** feature offers users a seamless way to transfer funds by scanning a QR code, removing the need for manual entry of account details. This process supports the generation, uploading, or scanning of unique QR codes to initiate or process transactions effortlessly. Follow these simple steps to complete a transaction:

1. **Access the Send Money Menu:**
   - Log in to your SBPay Mobile App.
   - Navigate to the **Send Money** menu and select the **SCAN QR** icon.

2. **Scan the QR Code:**
   - Point your device's camera at the static QR Code provided by the recipient.
   - Once the mobile app recognizes the QR Code, the system will automatically identify the recipient's account details, such as the account number.

SBPay Send Money (P2P) via Scan QR

1. Send Money   2. Scan QR   3. QR Code

www.southbankinc.com
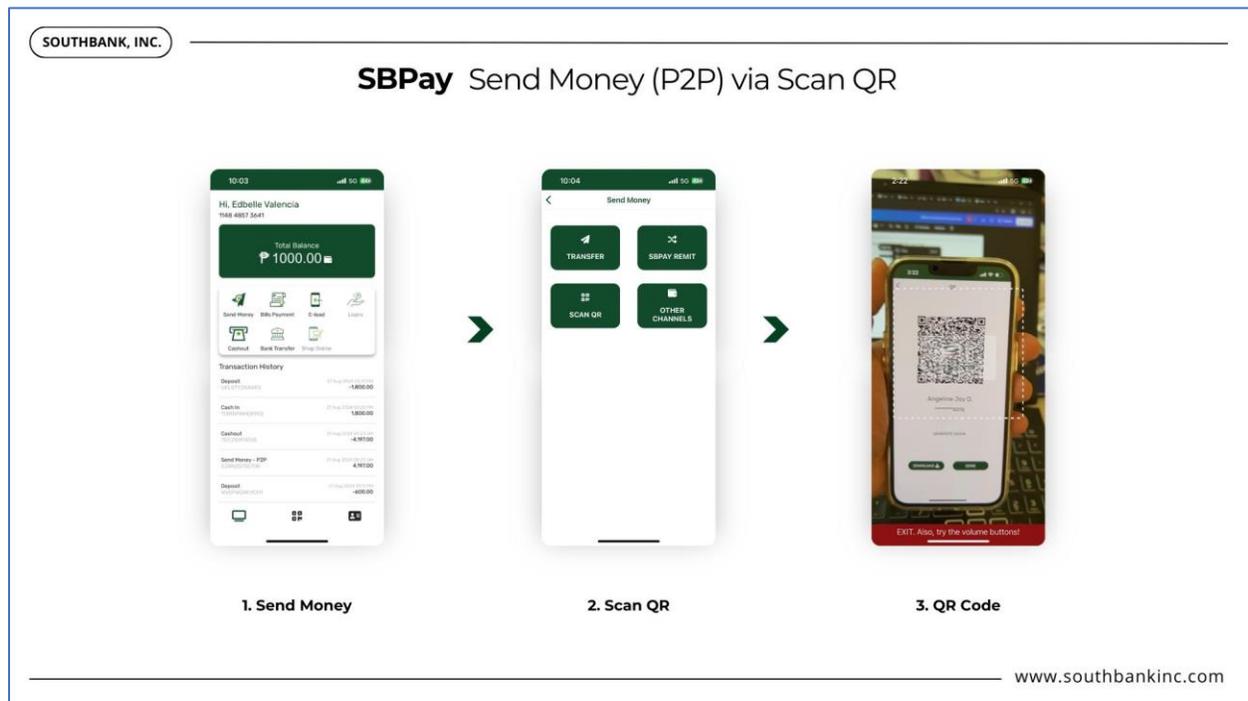
3. **Confirm Transaction Details:**
   - Review the automatically populated transaction details, which include:
     - **Account Number**
     - **Account Name (Receiver)**
     - **Amount to be sent**
     - **Fee**
     - **Total**
   - Verify the accuracy of these details.

4. **Initiate the Transaction and OTP**
   - Tap the **Send** button to complete the transfer.
   - The system shall push a **one-time PIN (OTP)** to confirm and proceed on the transaction.

5. **Transaction Summary:**
   - Upon successful completion, the system will display a summary of the transaction.
   - Users may choose to save or download this summary for reference.

4. Confirmation   5. Provide OTP   6. Summary/Notification
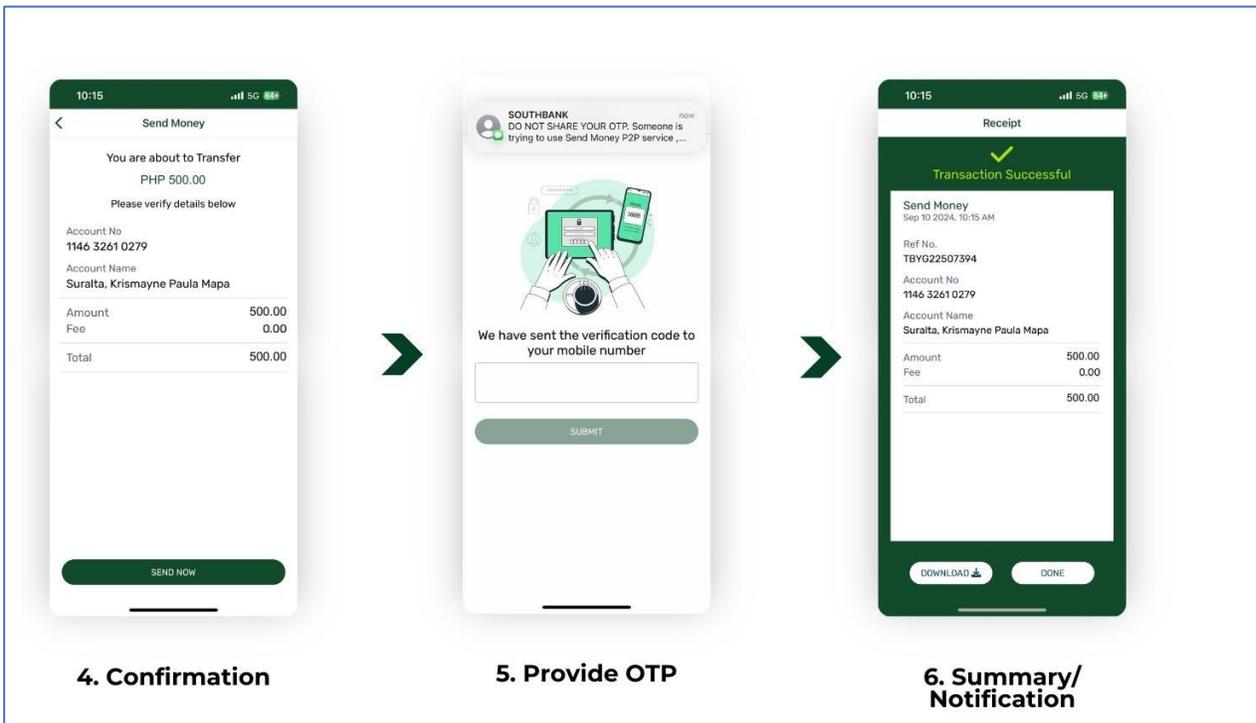
Benefits of the QR Code Feature:

- **Convenience:** Eliminates manual entry of recipient details, reducing errors.
- **Speed:** Speeds up the transaction process with a few simple steps.
- **Accuracy:** Ensures accurate recipient information through automated data capture.

The QR Code feature enhances the SBPay user experience by providing a secure, efficient, and user-friendly option for sending money.

GUIDELINES (SECTION 4.5):

To ensure seamless fund transfers using the SBPay mobile app, users must adhere to the following standard guidelines:

1. Login Verification
- Securely log in to the SBPay mobile banking app using your unique credentials (username and password, PIN code, or biometric login).
- This step ensures that only authorized users can initiate transactions.

2. Internet Connectivity and Fund Availability
- Ensure a stable internet connection throughout the transaction to prevent interruptions.
- Verify sufficient funds in your account before initiating the transaction.
- The system will automatically check your account balance to confirm fund availability.

3. Insufficient Funds Handling
- If your account has insufficient funds to cover the transaction, the system will halt the process.
- A notification will alert you of the issue, allowing you to address the balance before proceeding.

4. Accuracy of Recipient QR Code:

- **Proper Scanning:**
    a) The client must ensure that the QR Code is scanned properly to guarantee readability and accuracy of the targeted account details.

- **Validation of QR Code:**
    a) The system will validate the scanned QR Code before processing.
    b) If the QR Code is invalid or unreadable, the transaction will be flagged, and the user will receive an appropriate notification or prompt to correct the issue.

- **Handling Mistaken Transfers:**

  a) If the client inadvertently transfers funds to the wrong account due to an error in the QR Code, they may file a dispute.
  b) Refer to *Attachment #1 - Technical and Operational Support Procedure* for the steps to request a manual transaction reversal.

5. Transaction Processing

a) After verification, the sender's account balance will be debited by the transfer amount, including applicable fees.
b) The receiver's account will be credited in real time, confirming a successful transfer.
c) Notifications will be provided to both parties to confirm transaction completion.

4.6 REAL TIME BANK TRANSFER VIA INSTAPAY OR ECCASH:

SBPay enables seamless and real-time funds transfer between various banks, empowering users to manage their finances effectively across multiple financial institutions.

Features and Options:

1. **Send or Transfer Funds via InstaPay:**
   - **InstaPay:**
     a) Provides instant fund transfers, ensuring the recipient receives the funds immediately.
     b) Ideal for urgent, low-value transactions with a maximum amount limit per transaction amounting to 50 thousand pesos.
     c) Available 24/7, including weekends and holidays.

2. **Secure and Efficient Transactions:**
   - Integrated with secure banking networks to ensure the safety and reliability of fund transfers.
   - Real-time updates and notifications on the status of transactions.
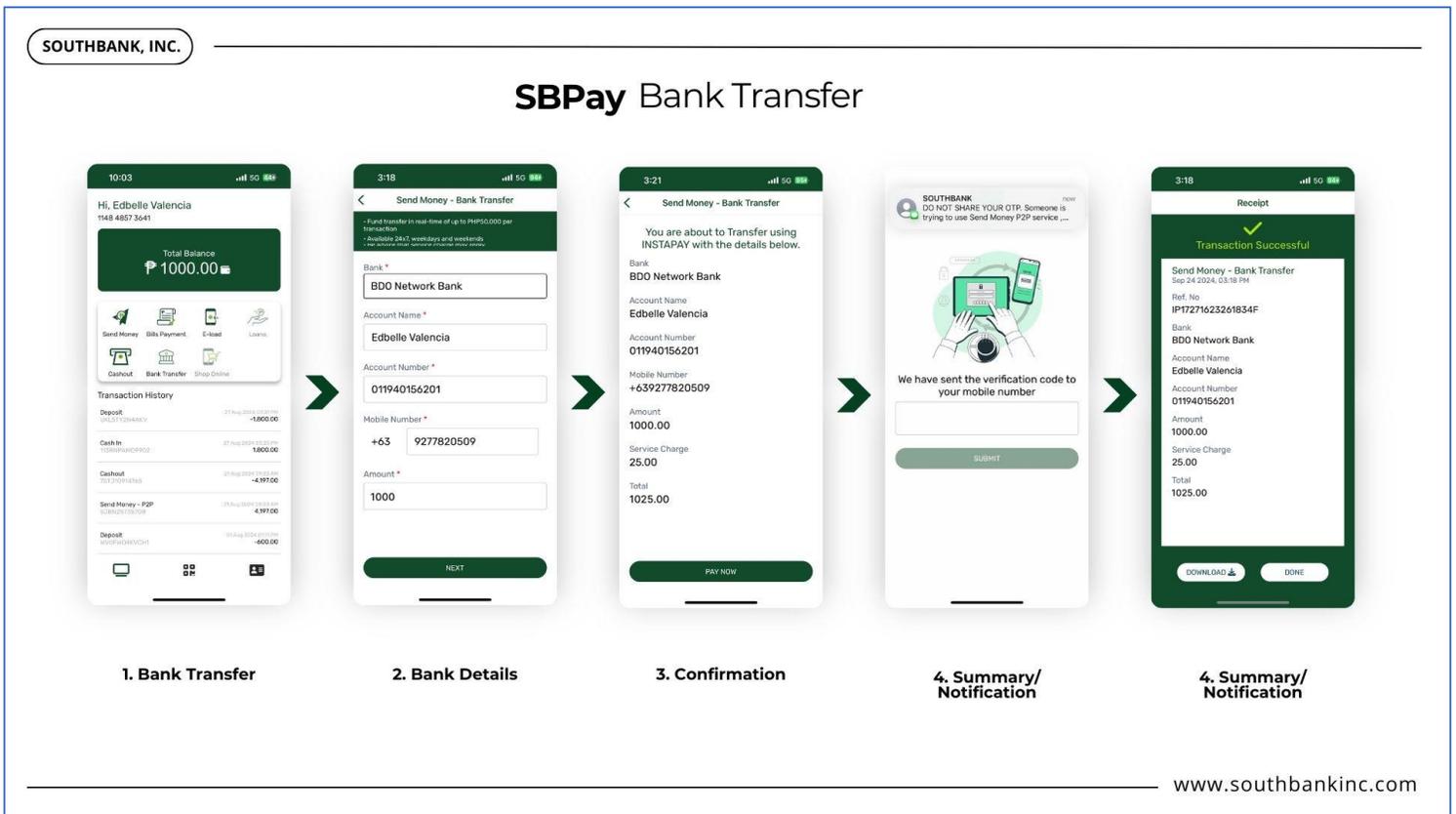
SOUTHBANK, INC.

SBPay Bank Transfer

1. Bank Transfer
2. Bank Details
3. Confirmation
4. Summary/ Notification
4. Summary/ Notification

www.southbankinc.com

OPERATIONAL GUIDELINES (SECTION 4.6):

1. **Accessing the Feature:**

   a) Login to the SBPay mobile app using secure credentials.
   b) Navigate to the "Bank Transfer" menu and select the target recipient institution based on your transaction requirement.

2. **Input Details:**

   a) Enter the recipient's bank name, account number, and the amount to be transferred.
   b) Confirm details, including applicable fees amounting to 25 pesos and total amount, to proceed.

3. **Transaction Confirmation Process**

   • **Verify Transaction Details:**

   a) Review the transaction summary displayed on the confirmation screen.
   b) Ensure all details, such as the recipient's name, account number, transfer amount, and fees, are accurate.

   • **Initiate the Transfer:**

   a) After verifying the details, click the **"Send"** button to proceed with the transaction.

   • **OTP Validation for Security:**

   a) An OTP (One-Time Password) is generated and sent to the user's registered mobile number or email.
   b) Input the received OTP into the designated field on the confirmation screen.

   • **Transaction Completion:**

   a) Once the correct OTP is entered and validated, the system processes the transaction.
   b) A notification confirming the successful transaction will be displayed, and the user may download or save the receipt for reference.
   c) An SMS and email notification shall be received by the client's number and email.

4. Fee Sharing and Configuration

- **Fee Configuration:**

  a) The service fee for transactions is managed and configured within the **Fee Management Module** under the control of the Head Office (HO)/Admin.

- **Service Fee Details:**

  a) A fixed service fee of **PHP 25** is applied per transaction.

- **Fee Distribution:**

  ▪ The collected service fee is shared between the Bank and I2I – UBX as follows:

  a) **PHP 15** is allocated to the Bank.
  b) **PHP 10** is allocated to I2I – UBX.

- **Settlement Process:**

  a) The entire service fee is fully settled in the Bank's account with UnionBank, ensuring accurate and timely allocation to the respective parties.

5 **Error Handling and Dispute Resolution:**

  a) Users report disputes via the SBPay customer support and file a ticket.
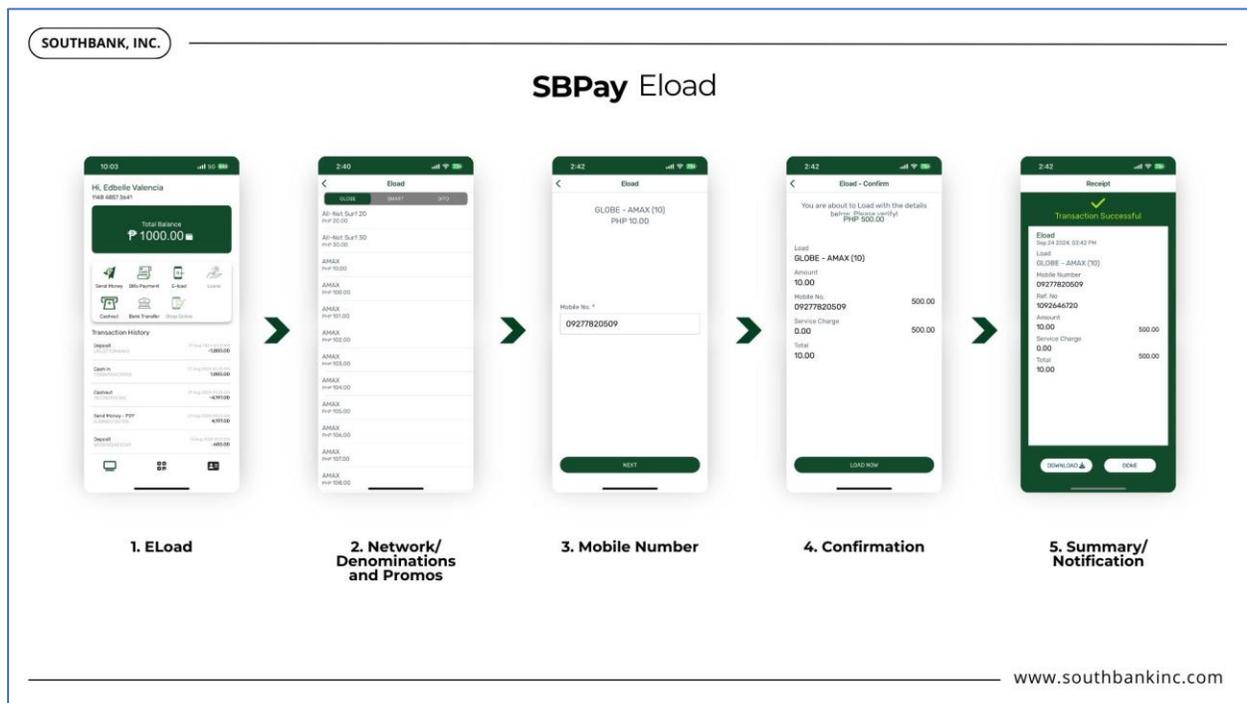 b) Refer to ***Attachment #1 - Technical and Operational Support Procedure***.

4.7 BILLS PAYMENT FACILITY

Bills Pay connects SBPay users to an extensive network of billers, simplifying bill management and payments directly within the app.

Functions:

1. **Connected to Over 150 Networks via ECPay:**

   - SBPay leverages integration with ECPay, enabling users to pay bills to more than 150 service providers.
   - Features include:
     a) Real-time retrieval of bill amounts.
     b) Instant payment processing and confirmation.
     c) Automatic generation of digital receipts for user convenience.
   - Ideal for utility, telecom, and other recurring payments, offering users a seamless and efficient experience.

2. **Direct Biller Integration:**

   - SBPay enables the onboarding of merchants not part of the ECPay network or other existing biller systems.
   - Through a straightforward registration process, these merchants can be integrated into SBPay for bill payments, expanding the platform's reach and flexibility.

   For additional information and guidance on Direct Biller Onboarding, refer to Attachment #6.

SOUTHBANK, INC.

SBPay Bills Payment (ECPay)

1. Bills Payment   2. Biller Category   3. Billers

www.southbankinc.com

SBPay Bills Payment (ECPay)

4. Account Details   5. Confirmation   6. Provide OTP   7. Summary/Notification
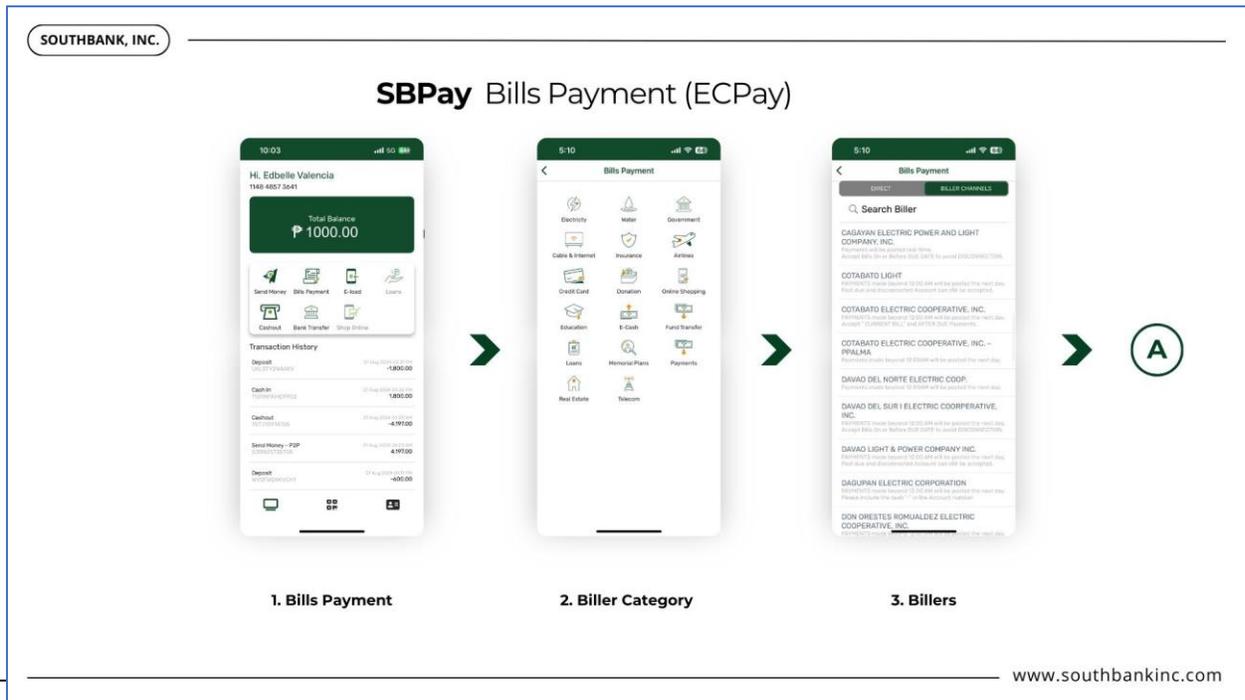
www.southbankinc.com
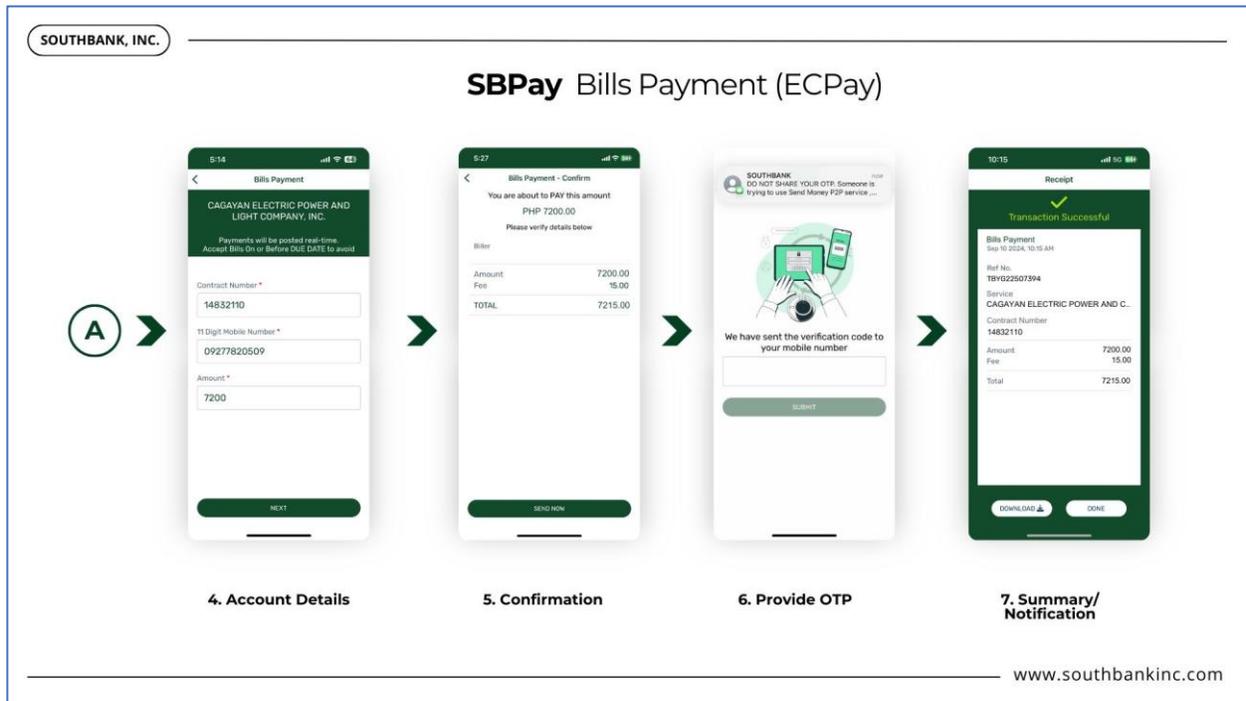
1. User Access

- **Login:** Users log in securely using their credentials to access the Bills Payment Facility.

2. Payment Processing

- **Select Biller:** Users choose a biller from the directory or enter details for a direct biller.

- **Enter Details:** Users input required information such as account/reference numbers and payment amounts.

- **Payment Confirmation:**

    a) System retrieves real-time bill information where applicable.
    b) Users review and confirm payment details.
    c) An OTP (One-Time Password) is generated and sent to the user's registered mobile number or email.
    d) Input the received OTP into the designated field on the confirmation screen.

- **Processing:**

    a) System deducts the payment amount from the user's SBPay account.
    b) System forwards the payment to the respective biller via ECPay or direct integration.

- **Receipt Generation:** Users receive a digital receipt/validation slip upon successful payment.

- **Error Handling and Dispute Resolution**
    - Users report disputes via the SBPay customer support and file a ticket.
    - Refer to *Attachment #1 - Technical and Operational Support Procedure*.

4.8 E-LOADING

The E-Loading feature empowers SBPay users to conveniently purchase prepaid mobile credits directly through the platform, ensuring fast and seamless transactions.

Function

Buy Load:

- Users can quickly and effortlessly purchase prepaid mobile credits for their own use or for others.
- The system integrates directly with telecom providers to validate and process transactions in real-time, ensuring instant load top-ups with minimal processing time.
- A confirmation message is sent to both the sender and recipient, providing transparency and assurance of successful transactions.

THE INFORMATION IN THIS DOCUMENT MAY NOT BE DISCLOSED WITHOUT THE PRIOR WRITTEN
CONSENT OF SOUTHBANK INC. | PRIVATE AND CONFIDENTIAL

Page | 25

OPERATIONAL GUIDELINES (SECTION 4.8):

1. **User Access**

   a) Login: Users securely log in to the SBPay platform using their credentials.
   b) Select E-Loading Option: Navigate to the "Buy Load" section in the app.

2. **Transaction Processing**

   - **Input Details:**

     a) Users select the telecom provider and enter the mobile number to load.
     b) Specify the desired load amount.

   - **Payment Confirmation:**

     a) The system deducts the corresponding amount from the user's SBPay account.
     b) The transaction is forwarded to the telecom provider for validation.

   - **Load Delivery:**

     a) Upon successful processing, the telecom provider credits the mobile number with the specified load.
     b) A confirmation message is sent to the user and the recipient.

4.9 CASHIN / DEPOSIT TRANSACTION

SBPay provides users with real-time deposit capabilities, offering seamless cash-in options across various channels to ensure funds are instantly available for transactions.

Function:

Deposit Money via Branches:

- Customers can deposit funds directly at bank branches or through P2P (SBPay-to-SBPay) fund transfers.
- Transactions are processed in real time, guaranteeing immediate availability of funds.
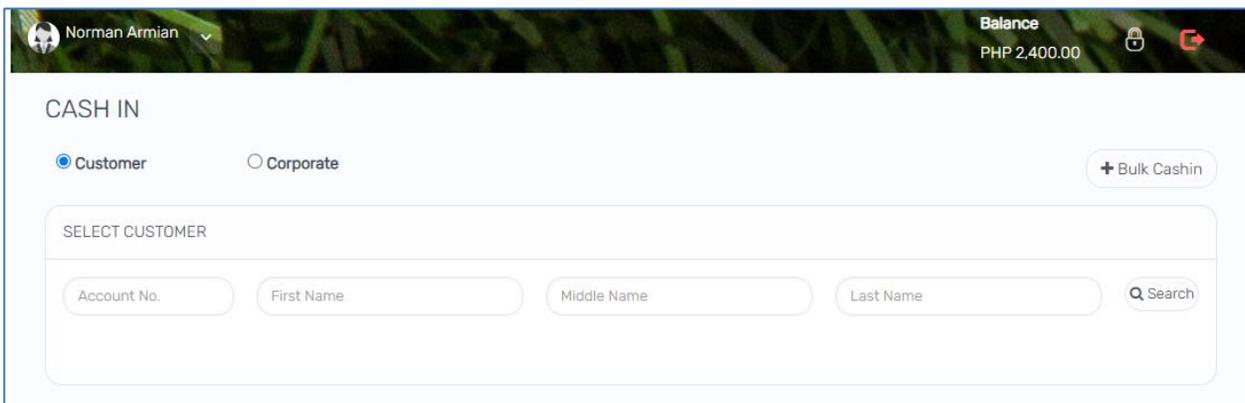
OPERATIONAL GUIDELINES (SECTION 4.9):

1. **Client Process:**

   - The client must complete the SBPay transaction form at the branch and provide the following details:
     a) **Account Number (Individual or Corporate/Business)**
     b) **Account Name**
     c) **Amount**

   Note: Cash-in/Deposit transactions are FREE.

2. **Branch Personnel Process:**

- Verify the accuracy of the details provided by the client by matching the account information in the system. This can either be an individual or corporate/business account.
- Upon successful validation and confirmation, accept the cash from the client and input the transaction into the system.

To process this transaction, please refer to the guide below:
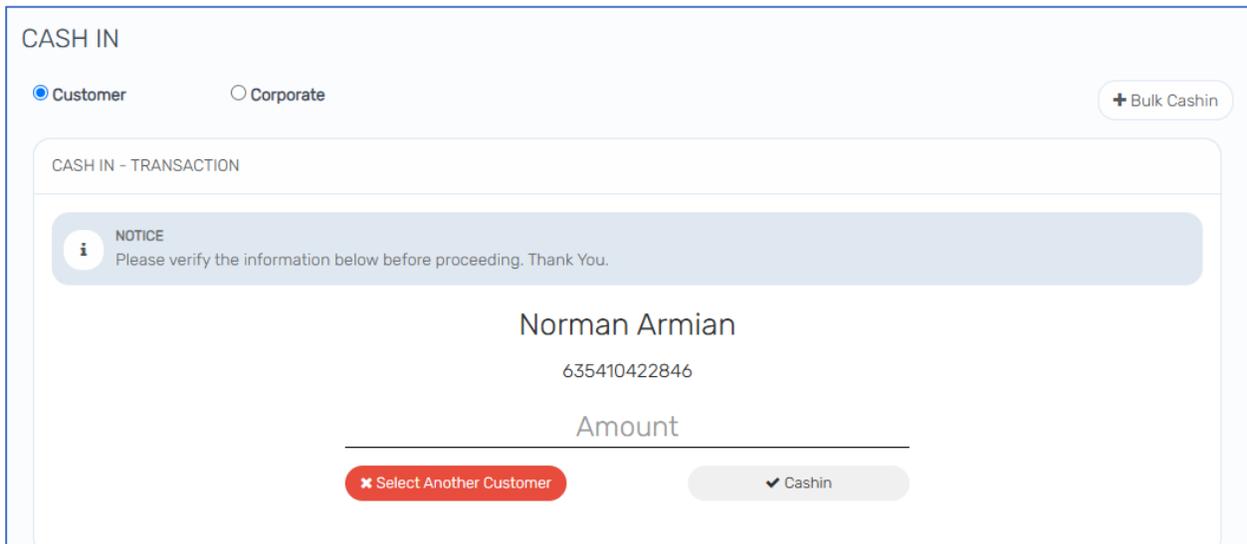
This module enables the branch personnel to choose from individual or business accounts.
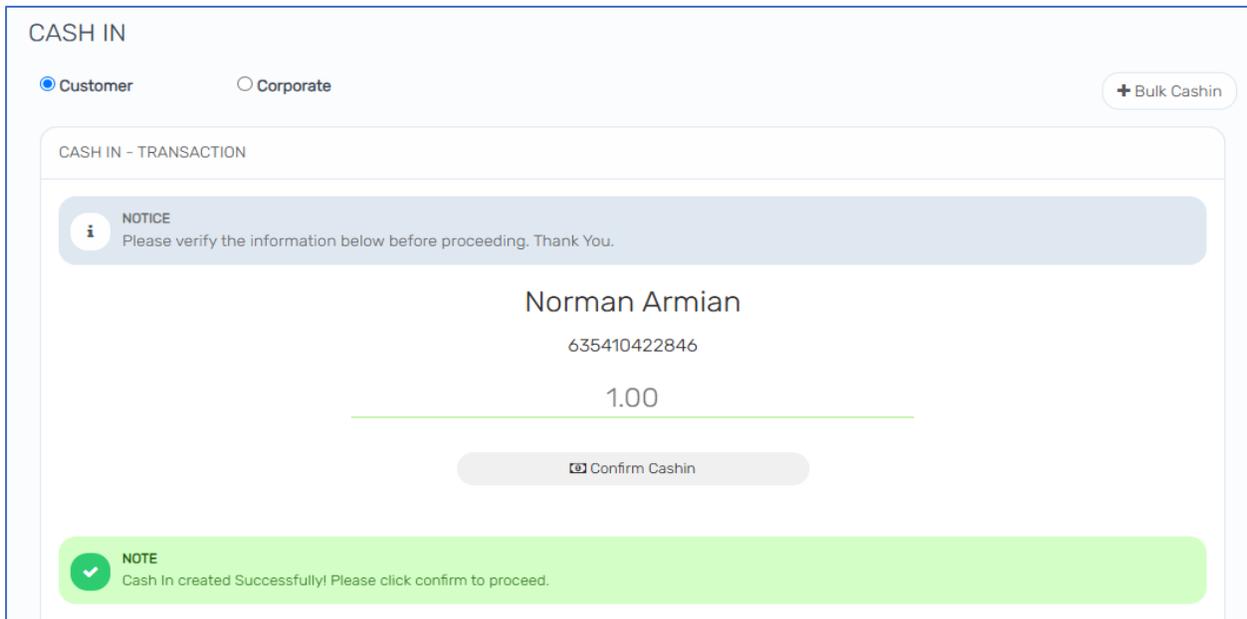
This module confirms the transaction details before proceeding.

- Once the transaction is processed, the client will receive an automatic notification (email & sms) confirming the successful deposit.

3. **Client Validation:**

   - The client can log in to their SBPay account to view and validate the transaction.

4. **Branch Personnel Validation:**

   - Branch personnel can verify the transaction by navigating the Statement of Account (SOA) or reviewing the Cash In/Deposit Transaction reports.
   - The system automatically generates a transaction report that can be printed and provided to the client as proof of the transaction.

5. **Automated Notifications:**

   - Once the transaction is processed, the system sends an **SMS** and **email notification** to the client confirming the successful deposit.

	NOTE	
✓	Cash In Success!	

DIGI UNIT BRANCH	Dec 09 2024, 09:35 pm	DIGI UNIT BRANCH	Dec 09 2024, 09:35 pm
Norman Armian	Refno: DIGIBRANCH0011621450	Norman Armian	Refno: DIGIBRANCH0011621450
09172473822		09172473822	
Name:	Norman Armian	Name:	Norman Armian
Amount:	1.00	Amount:	1.00
Fee:	0.00	Fee:	0.00
Discount:	0.00	Discount:	0.00
Total:	1.00	Total:	1.00
Previous Balance:	93.71	Previous Balance:	93.71
Current Balance:	94.71	Current Balance:	94.71
Customer's copy		**Branch's copy**	

Print Receipt

This module signifies a successful transaction. A copy of a validation slip is generated.

4.10   CASH OUT / WITHDRAWAL

SBPay provides users with multiple cash withdrawal options, ensuring flexibility and security for those needing quick and reliable access to their funds.

Function:

1. **Withdraw via Reference Code:**

   a) Users can generate a secure reference code through the SBPay platform for cash withdrawals.
   b) The reference code can be presented at branches or partner agents for processing.
   c) The system verifies the reference code and associated account details to ensure a secure transaction before releasing funds.

2. **Withdraw via Account Number:**

   a) Customers may withdraw funds directly using their account number.
   b) The system validates the withdrawal request in real-time, ensuring that sufficient funds are available for immediate disbursement.

THE INFORMATION IN THIS DOCUMENT MAY NOT BE DISCLOSED WITHOUT THE PRIOR WRITTEN
CONSENT OF SOUTHBANK INC. | PRIVATE AND CONFIDENTIAL

Page | 30
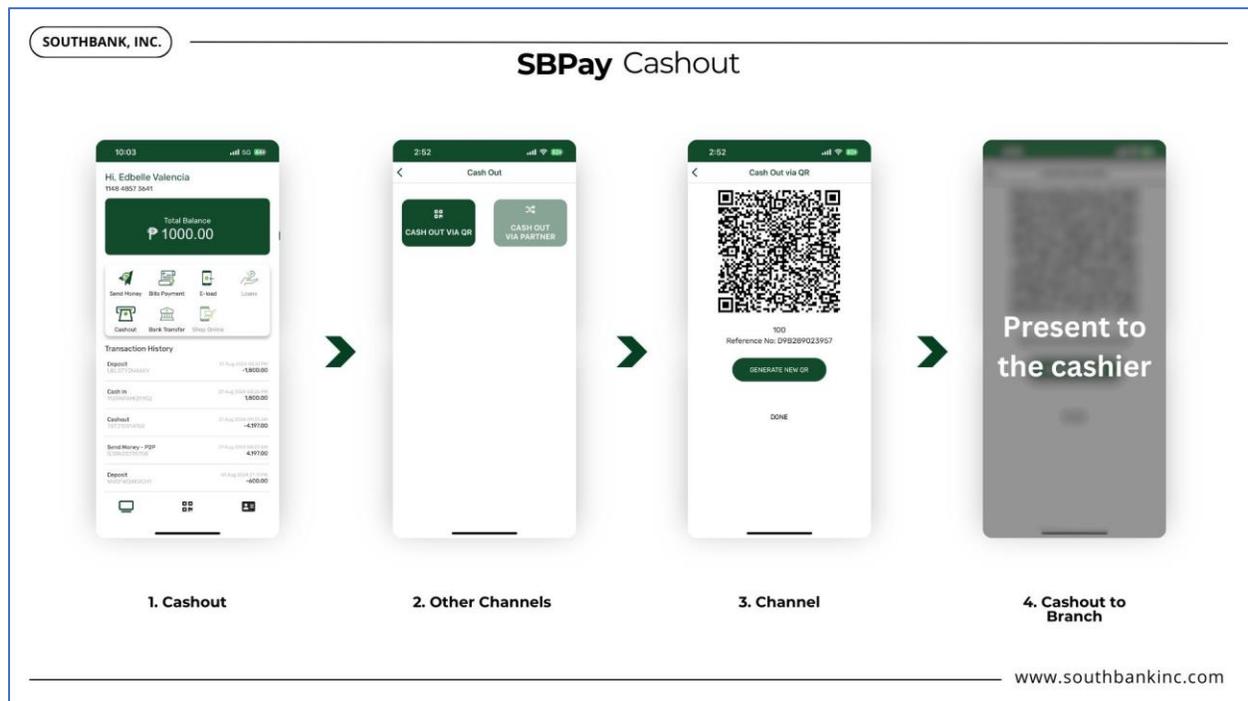
OPERATIONAL GUIDELINES (SECTION 4.10):

1. **Generating a Reference Code (For Reference Code Withdrawals):**

   a) The client logs in to their SBPay account and navigates to the **Cash Out/Withdrawal** section.
   b) Select the option to generate a **Reference Code** and input the desired withdrawal amount.
   c) A unique code is created. This reference code shall be presented to the branch personnel during the transaction.
   d) The reference code is valid for 2 hours, after which it will automatically expire. This time-bound validity serves as a security measure to ensure the transaction is completed promptly and to mitigate potential risks associated with unauthorized use.

2. **Withdrawing Funds at Branches:**

   a) The client presents the reference code or provides their account number along with valid identification. A cash-out form is available in the branch to proceed with the transaction.
   b) The branch personnel or agent verifies the reference code or account details using the system. This process includes accessing the client's information, such as their registered ID and photo, ensuring accurate identification and secure processing of the withdrawal.
   c) Once validated, the cash is disbursed to the client.

3. **System Verification and Notifications:**

   a) The system checks for sufficient funds and account authenticity before processing the withdrawal. The system will not allow if the fund is not sufficient to proceed with the transaction.
   b) After completing the transaction, the system generates a receipt and sends SMS/email notifications to the client for confirmation.
   c) A flat fee of 10 pesos is applicable regardless of the amount.

4. **Monitoring and Reporting:**

   - Both the client and branch personnel can view the transaction via the system's **Statement of Account (SOA)** or the **Cash Out/Withdrawal Reports** for transparency and validation.

BRANCH AND HEAD OFFICE OPERATIONS

5. PREFUNDING PROCEDURE (ECPAY, I2I AND SBPAY WALLET FUNDING)

The prefunding procedure facilitates the transfer of funds from the settlement accounts of partner aggregators (ECPay and i2i) to enable the SBPay facility to process services via the aggregators' APIs. Without sufficient funds in the ECPay or i2i wallet, the system will be unable to process transactions such as bill payments and fund transfers.

OPERATIONAL GUIDELINE (SECTION 5):

1. Request for Fund Loading:

a) Finance personnel deposits the required funds into the settlement accounts of ECPay or i2i.
b) The transaction is monitored until the funds are reflected in the aggregator's balance.

2. Request for Fund Loading:

a) Once the funds are confirmed in the settlement account, head office finance personnel initiate a request to load these funds into the SBPay Wallet or Fund Management system.
b) The request is processed via the designated system interface.

3. Approval by System Admin:

To ensure transparency and due diligence during the pre-funding process with external providers (ECPay, i2i), the prefunded balance must be formally requested by the Head Office (HO) Finance Head to the system admin. This balance should be accurately reflected in the SBPay Mother Wallet Account.

The following procedures must be observed:

a) **Request Submission** – The HO Finance Head shall submit a formal request for pre-funding, specifying the required amount and intended usage.

b) **Verification and Approval** – The request will undergo internal verification to ensure compliance with financial policies and sufficient fund allocation.

c) **Balance Reflection** – Upon approval, the prefunded amount will be credited and reflected in the SBPay Mother Wallet Account.

d) **Monitoring and Reconciliation** – Through the attached deposit slip during the request process, regular monitoring and reconciliation will be conducted to track fund movements and maintain accurate records.

4. **Disbursement to Branch Wallets:**

   a) The head office finance disburses the necessary funds to the respective branch wallets based on the request for operational requirements. As a standard procedure, a fund request is to be made using the system interface along with the request attachment detailing the purpose/use of the funds.
   b) This fund enables SBPay to execute services such as transactions, bill payments, and fund transfers efficiently.

5. **Fund Request and Management**

   a) The Finance Unit oversees the allocation of funds and monitors wallet balances to ensure continuous transactional capabilities for SBPay operations.
   b) A Daily Balance Report is prepared by the Settlement Unit and submitted via email by 4 PM cut-off. This report includes the available balance for each wallet or fund management system.

6. **Threshold Monitoring System:**

   a) The SBPay system has a threshold feature that alerts branches when their wallet balance falls below ₱50,000.
   b) This notification ensures timely action by the branch to request additional funding, preventing transaction disruptions.

7. **Branch Fund Request Process:**

   a) Branches must submit fund requests through the system along with the attached prescribed Requisition Form detailing the purpose of the request.
   b) The request must include:
      - The purpose of the request and proper approval.
      - Details of fund allocation and the requested amount.
      - Required attachments, such as supporting documentation.

8. **Fund Request Validation and Approval:**

   a) The Finance Unit, acting as the fund manager, evaluates submitted requests and may approve or deny requests under the following conditions:

      1) Missing or improper approval from the Branch Officer.
      2) Absence of a summary of fund allocation or stated purpose.
      3) Discrepancies in the attached documentation.
      4) Required alterations to the requested amount as communicated by the Finance Unit.
      5) Situations requiring further validation due to questionable circumstances.

9. **Fund Management and Control:**

- The Finance Unit retains the authority to control or adjust fund requests under the following conditions:

    a) Liquidity concerns affecting the bank's financial health.
    b) Priority transactions that require immediate fund allocation over regular requests.
    c) Exceptional circumstances warranting resource reallocation to maintain operational efficiency.

For reference on the system flow, please refer to the following procedures:

➢ **BRANCH PORTAL (REQUEST):**
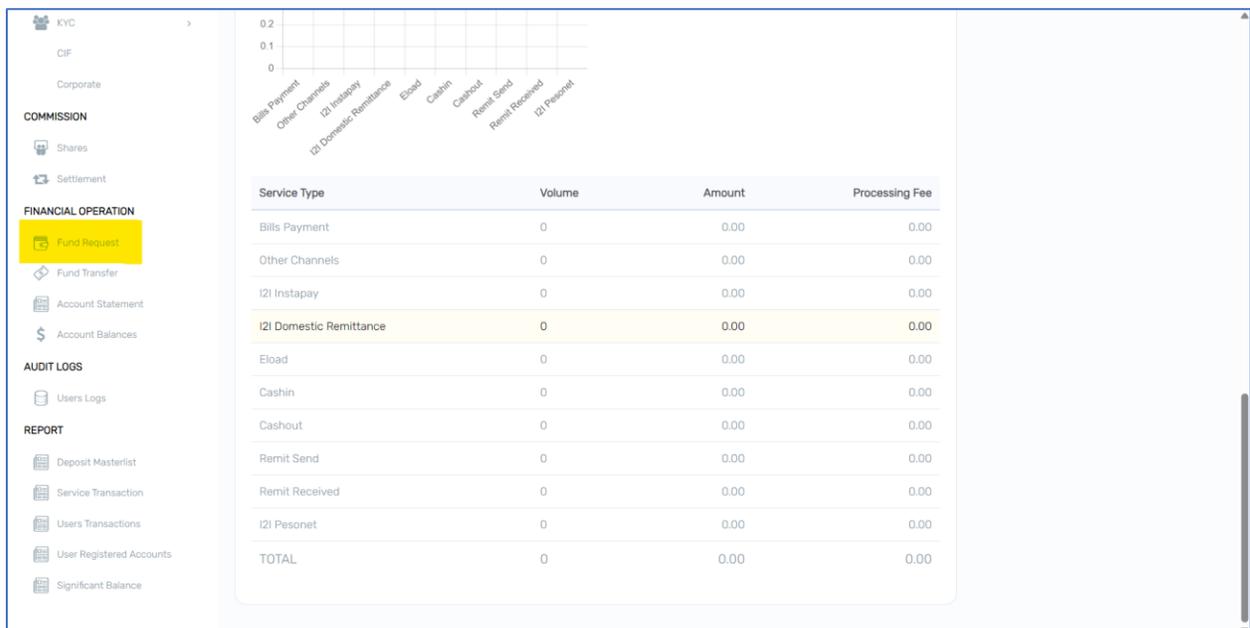
Log in to your Corporate Maker Account and open Fund Request from the side menu.

Select Fund Request.

Enter the necessary details, and afterward click Fund Request.

THE INFORMATION IN THIS DOCUMENT MAY NOT BE DISCLOSED WITHOUT THE PRIOR WRITTEN
CONSENT OF SOUTHBANK INC. | PRIVATE AND CONFIDENTIAL

Page | 35
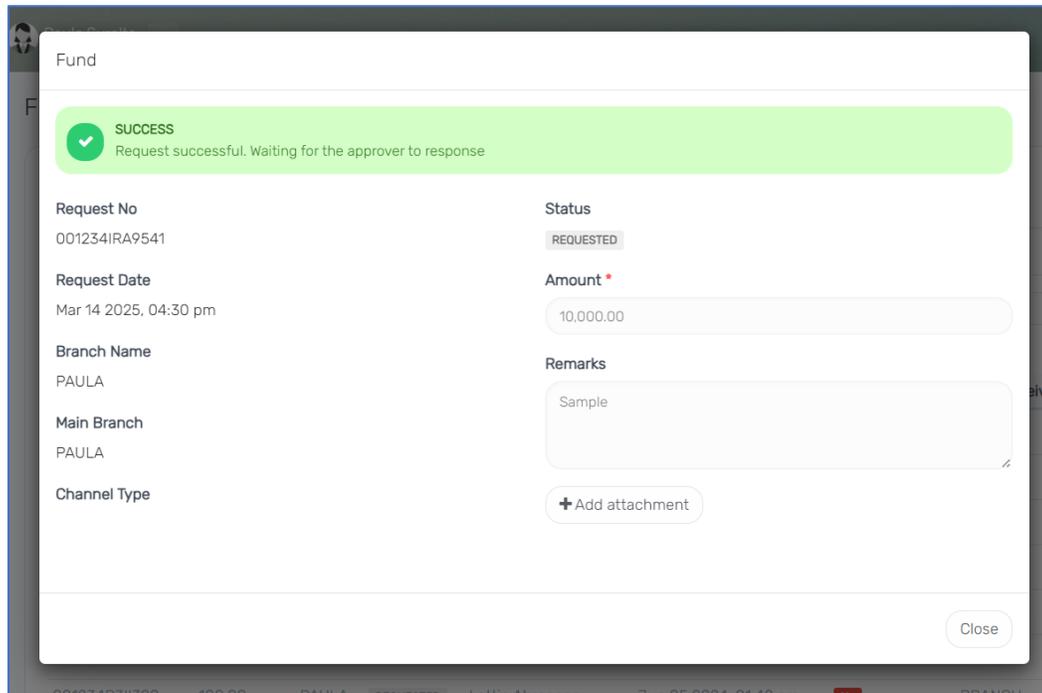
You can add necessary attachments after submitting a request.

➢ **HO PORTAL (APPROVAL):**
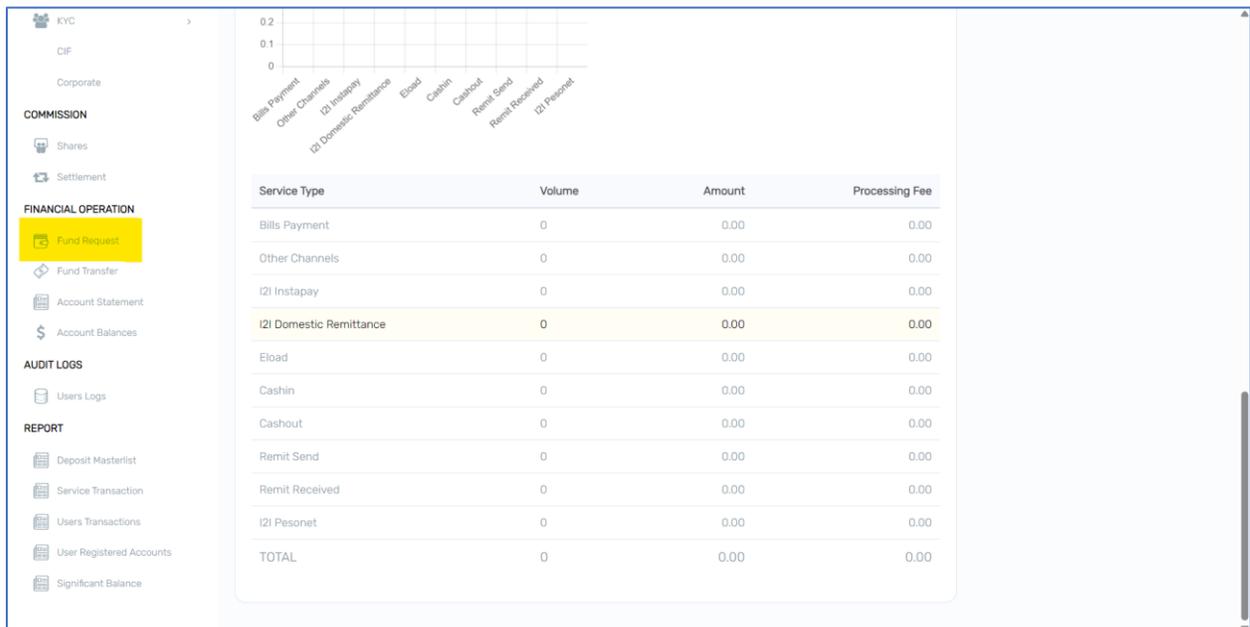
Log in to your Corporate Approver Account and select Fund Request from the side menu.

Click view on the targeted request.

Select whether to Approve or Reject a Fund Request.

Fund

⊗	**REMINDERS**
	You are about to **APPROVE** the below request. Please fill the asking details.

Request No
001234IRA9541

Request Date
Mar 14 2025, 04:30 pm

Branch Name
PAULA

Main Branch
PAULA

Channel Type

Status
REQUESTED

Amount *
10,000.00

Remarks
Sample

[⊡ Approved]   [✖ Reject]

Please enter your Password to approve the transaction *

Remarks

Confirm

Enter your password and remarks to confirm the action.

6. **STANDARD BRANCH DAILY OPERATIONS**

➢ **Start of Day Process**

6.1 Cashier Log-In:

a) The cashier logs into the SBPay system to prepare for the daily operations.
b) The system displays the branch wallet balance, already settled during the previous end-of-day process.

6.2 Transaction Processing

a) Transaction Documentation: All branch transactions conducted via SBPay services must be documented using the **SBPay Transaction Form.** This form is applicable in the following services such as Bills Pay, Cashin/Deposit, Cashout/Withdrawal, Eloading, Remittance, and Bank Transfers.
b) This form serves as the basis for transaction validation and processing.

Refer to Attachment #7 – SBPay Forms.

➢ **End of Day Process**

a) System-Generated Reports: At the end of the day, the system generates real-time transaction reports summarizing all activities performed.
b) Reports include:
   - Statement of Account (SOA) summarizing daily transactions.
   - SBPay Transaction Forms for each individual transaction.

6.3 Validation and Approval Workflow:

   - Reports and receipts are attached and verified by the following personnel:
     a) Teller: Maker
     b) Cashier: Checker
     c) BOO/BM: Approver

6.4 Submission to Accounting:

   - Once verified and approved, all reports are submitted to the branch accounting unit for proper recording and entry into accounting records.

- **All Reports can be generated from the REPORT category in the side menu.**
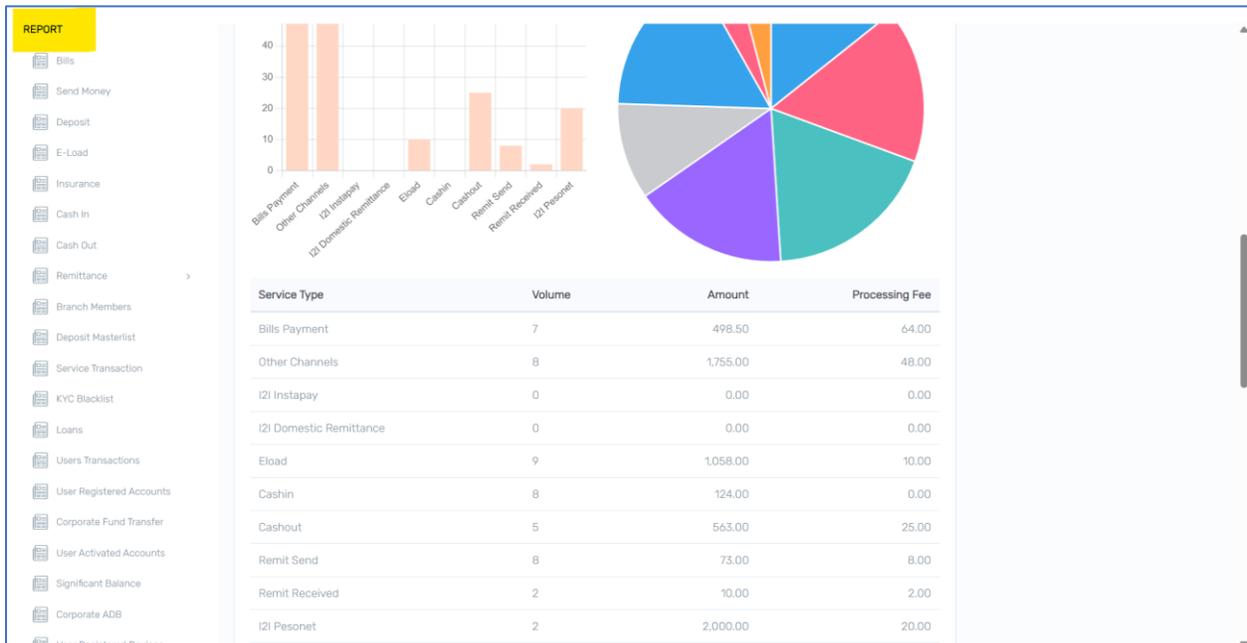
You can check all viewable reports on the Report Side Menu.
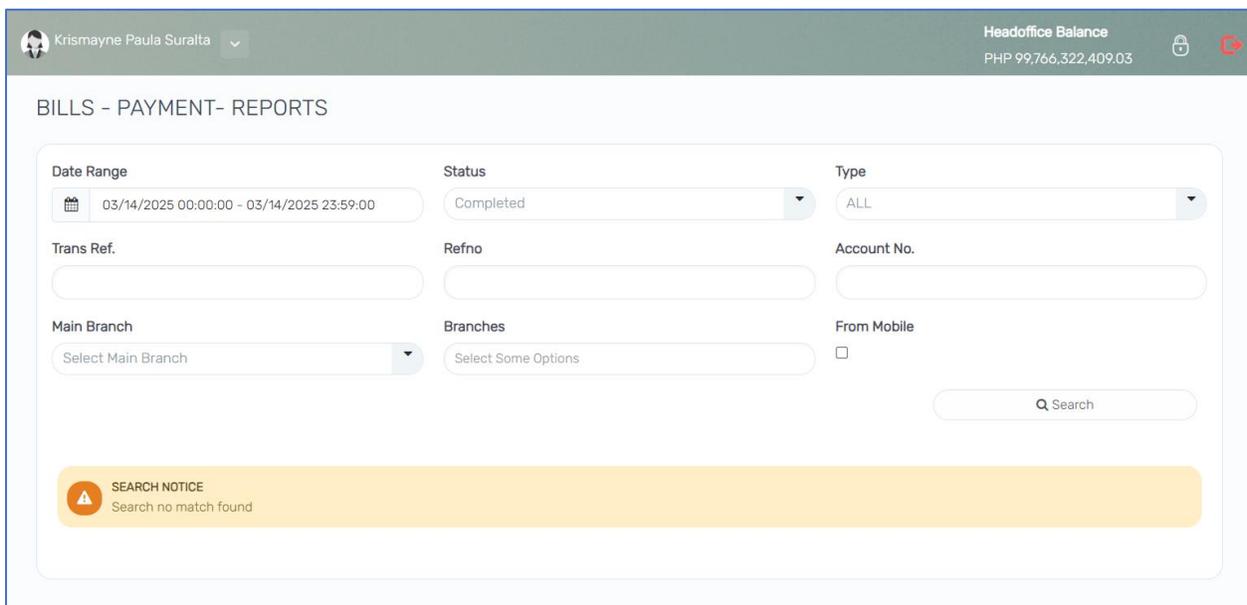
When checking for reports, Supply the necessary parameters and then click search.

7.0 MERCHANT ACCOUNT / ONLINE BUSINESS BANKING (OBB) ACCOUNT

The **Merchant/Business Banking Account** is an online dedicated platform designed to help business entities efficiently manage and facilitate their financial transactions. It provides a suite of essential services, including:

- **Bills Payment** – Conveniently settle utility bills, supplier payments, and other obligations.
- **Bank Transfers** – Securely transfer funds between accounts and financial institutions.
- **Disbursement** – Streamline employee salary payments with automated processing.
- **Cash In/Cash Out** – Manage fund deposits and withdrawals with ease.
- **Balance Viewing** – Monitor account balances for transactions related to pickup deposits, settlements, and merchant activities.

This portal enhances financial management for businesses, offering a seamless, secure, and efficient online banking experience. This account is a regular savings account earning interest based on Average Daily Balance (ABD).

This account operates under a maker-checker (maker and approver) structure, where all transactions— such as bills payment, fund transfers, e-loading, and other service types—must undergo an approval process before any request initiated by the maker is completed.

1. Access and Customization:

> The portal's services and features are enabled based on the agreed-upon terms and functions during account setup. This can be filled in the business banking form.

> *Refer to Refer to Attachment #7 – SBPay Forms or https://southbankinc.com/business/*

a) Details of the services and limitations are outlined in the agreement signed by the business entity and the Bank.

2. Account Opening and Creation Requirements

a) **Eligibility**

- Any business entity is qualified to open an account, provided that all requirements are met.

THE INFORMATION IN THIS DOCUMENT MAY NOT BE DISCLOSED WITHOUT THE PRIOR WRITTEN
CONSENT OF SOUTHBANK INC. | PRIVATE AND CONFIDENTIAL

Page | 41

b) **Document Submission**

- Businesses must submit the required documents through a designated branch or an authorized bank representative.
- All forms must be duly completed and signed as per the provided guidelines.

   *Refer to Refer to Attachment #7 – SBPay Forms or https://southbankinc.com/business/*

    Refer to Refer to Attachment #7 – SBPay Forms or https://southbankinc.com/maker/ and https://southbankinc.com/approver/

c) **Processing & Account Creation**

- Upon submission, the complete set of documents and forms will be forwarded to the Head Office (Settlement/Digital Unit) for processing.
- The Settlement Unit will initiate account creation using the designated system tool.

3. Account Activation & Notification

- Upon successful account creation, access details will be sent to the client via their registered email.

- The email will include the assigned username, a temporary password, and the link to the portal for accessing the merchant or business account.

- A separate confirmation notification will be sent to the client via email, advising them of the account activation.

- The branch's official email will also receive a notification containing the details of the newly created account such as the account name and the account number.

- The client may nominate their preferred passwords for both the maker and approver roles during the initial login.
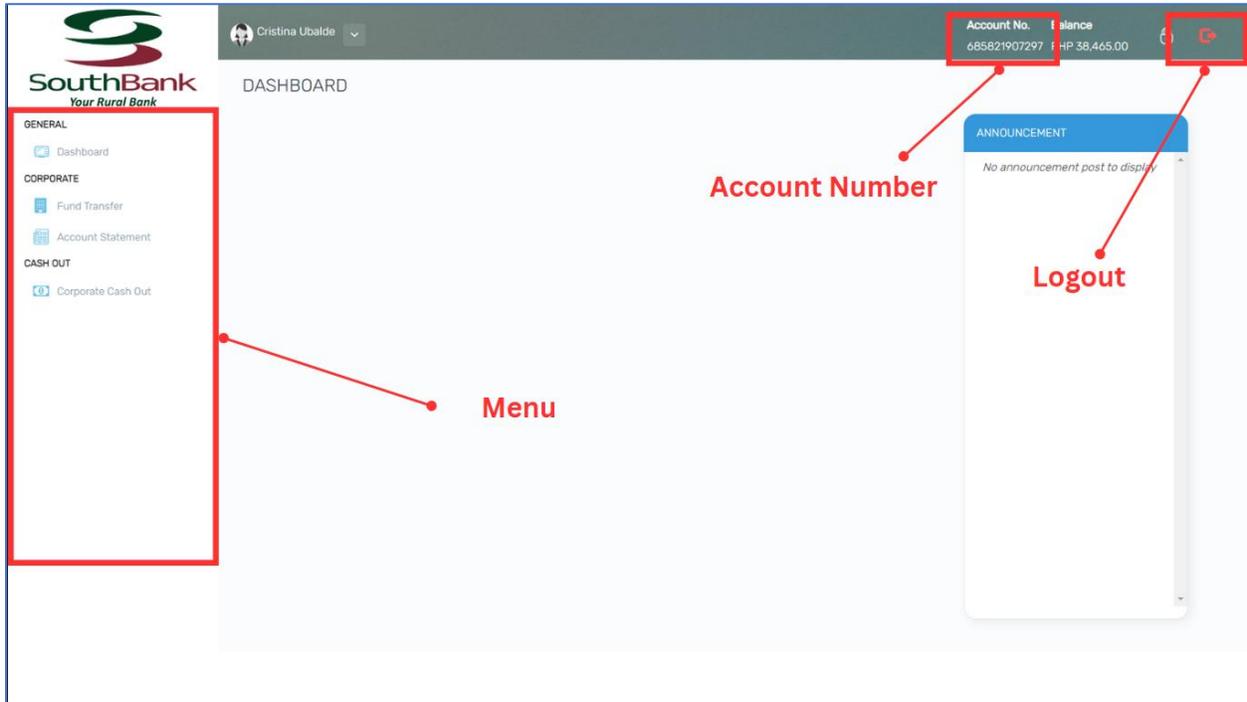
This shows the dashboard of the OBB Account upon successful login.

**7.1 MERCHANT / OBB ACCOUNT SERVICE TYPES:**

1. **SBPAY FUND TRANSFER (P2P)**

The Fund Transfer feature enables a merchant or online business banking (OBB) account to transfer funds to another SBPay merchant or business account. To ensure due diligence and security, this feature is equipped with a maker and approver workflow, requiring every initiated transaction to undergo a review and approval process.

Once the maker submits a fund transfer request, the approver will automatically receive an email notification containing the link to the pending transaction. After reviewing the transaction details, the approver may approve the request by clicking the *Approve* button and confirming the action through password authentication.

A fund transfer will only be completed if the following conditions are met:

   a) The merchant account has sufficient balance.
   b) The receiver's account is correct and active.
   c) The transaction is duly approved by the designated approver.

Additionally, this facility provides access to transaction reports, which are available in the account's Statement of Account for monitoring and reconciliation purposes.
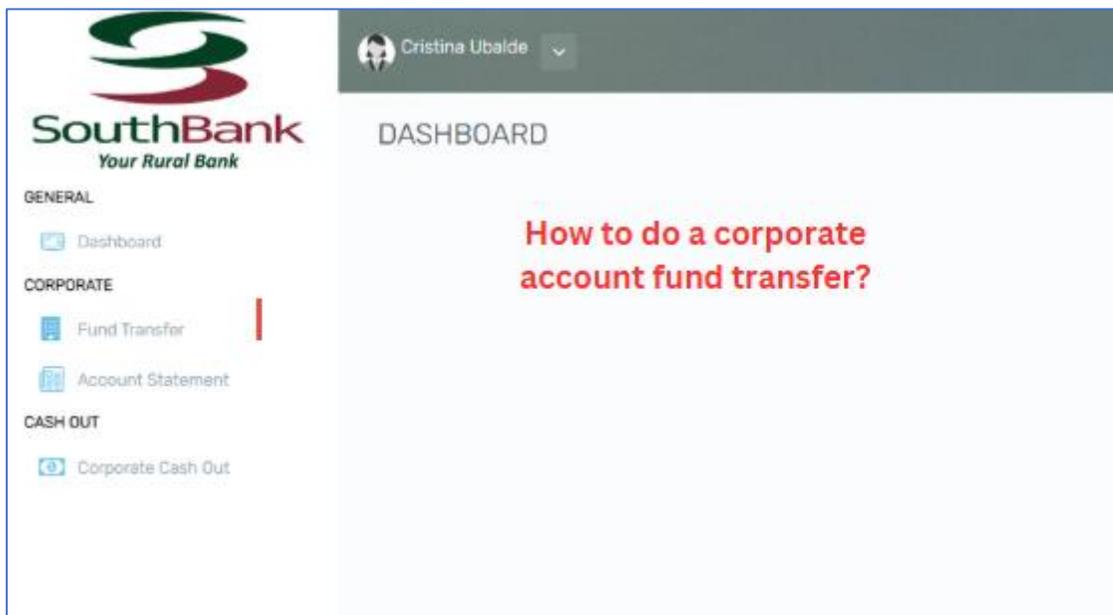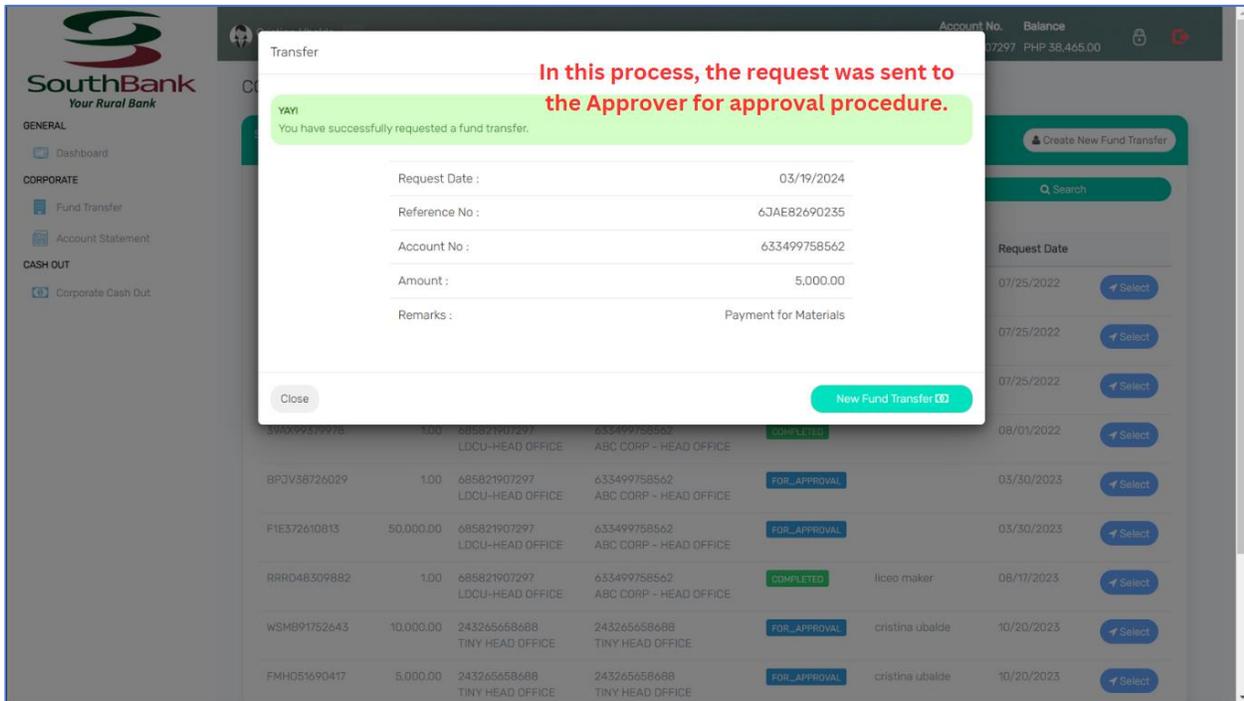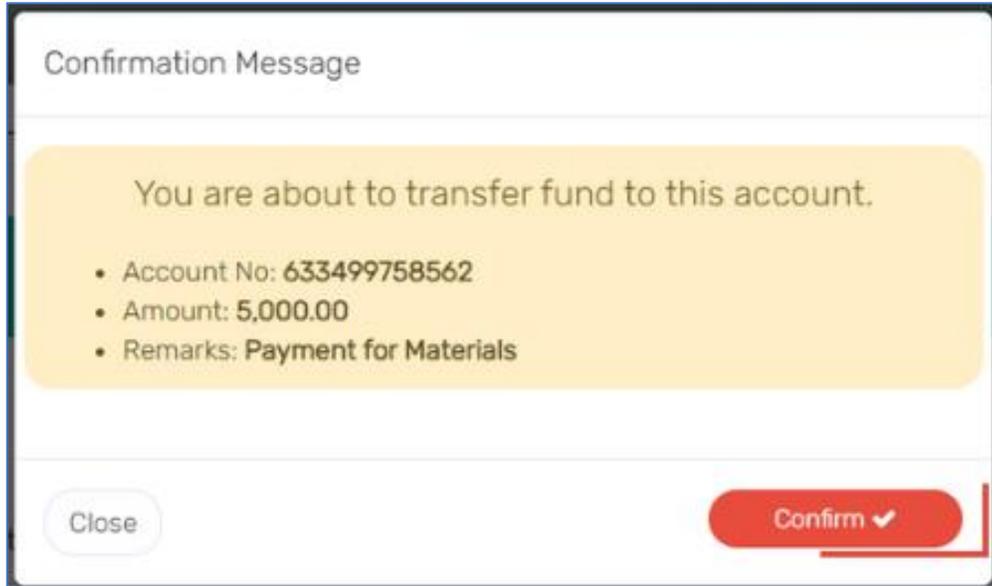

On this portal, the maker role initiates the fund transfer transaction (P2P) using the Fund Transfer menu.
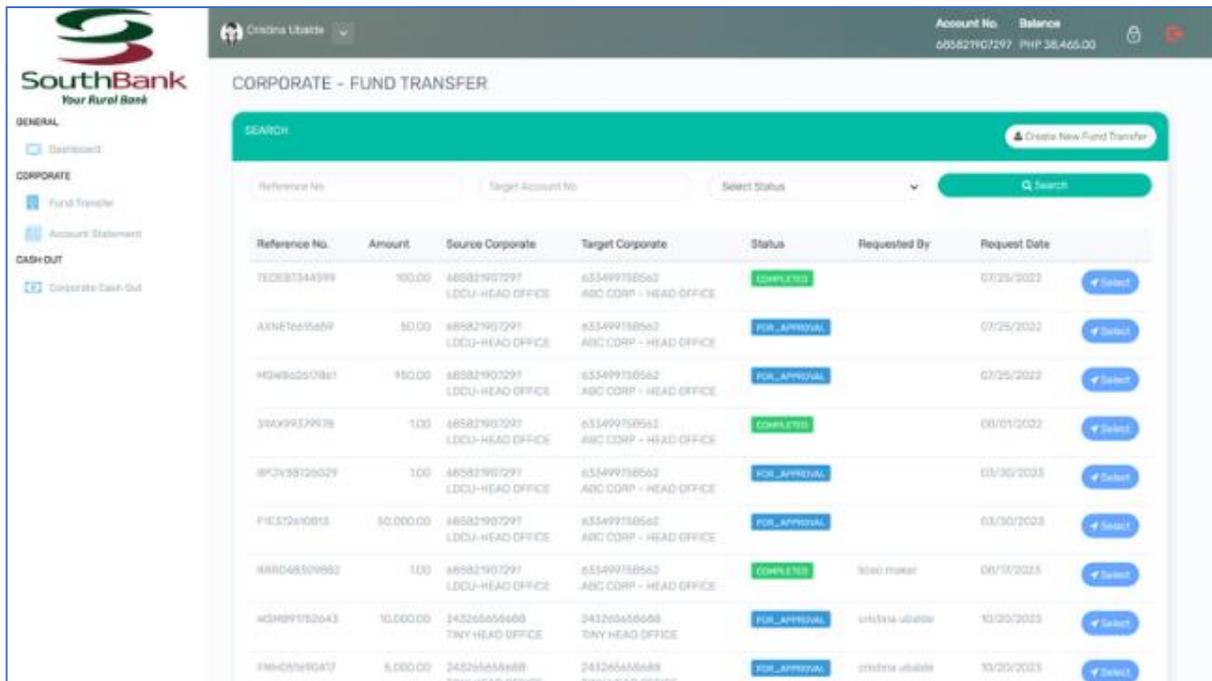
This user interface shows the navigation for the creation or initiation of the fund transfer transaction (P2P).
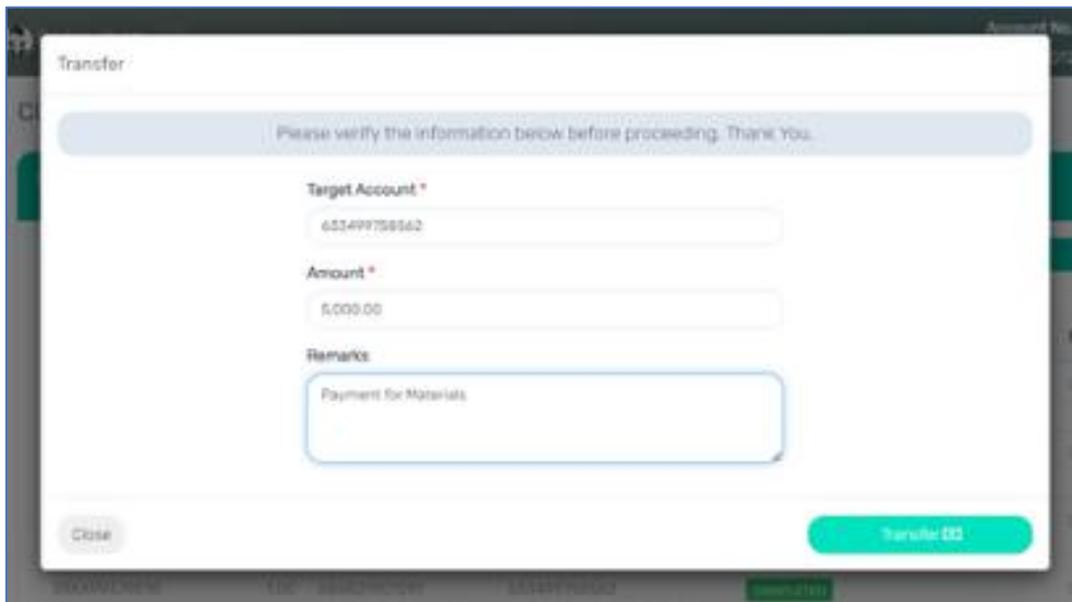
This displays the target account where the fund transfer will be received, along with other specific details.

2. **CASH-IN/DEPOSIT TRANSACTION:**

This process facilitates seamless deposit transactions into individual accounts, supporting both single and batch transactions. Designed for efficiency, this facility is particularly beneficial for payroll services, ensuring timely and accurate fund disbursement. By leveraging this system, businesses can streamline payroll processing, minimize manual intervention, and maintain transaction accuracy while ensuring compliance with banking standards.

Process Flow:

- **Transaction Initiation:** The transaction maker initiates the deposit transaction through the Business Account Portal. Once submitted, the request is forwarded for the approver's review.

- **Approval Procedure:** The approver reviews the request using the designated approval tool. To authorize the transaction, the approver must input a password and a one-time password (OTP) for verification.

- **Transaction Fulfillment:** Upon approval, the transaction appears in the maker's account via the Customer Transaction Module, where it must be confirmed to proceed.

- **Notifications:** Notifications are sent at each stage of the process—to the maker and approver—ensuring transparency and timely updates on transaction status.
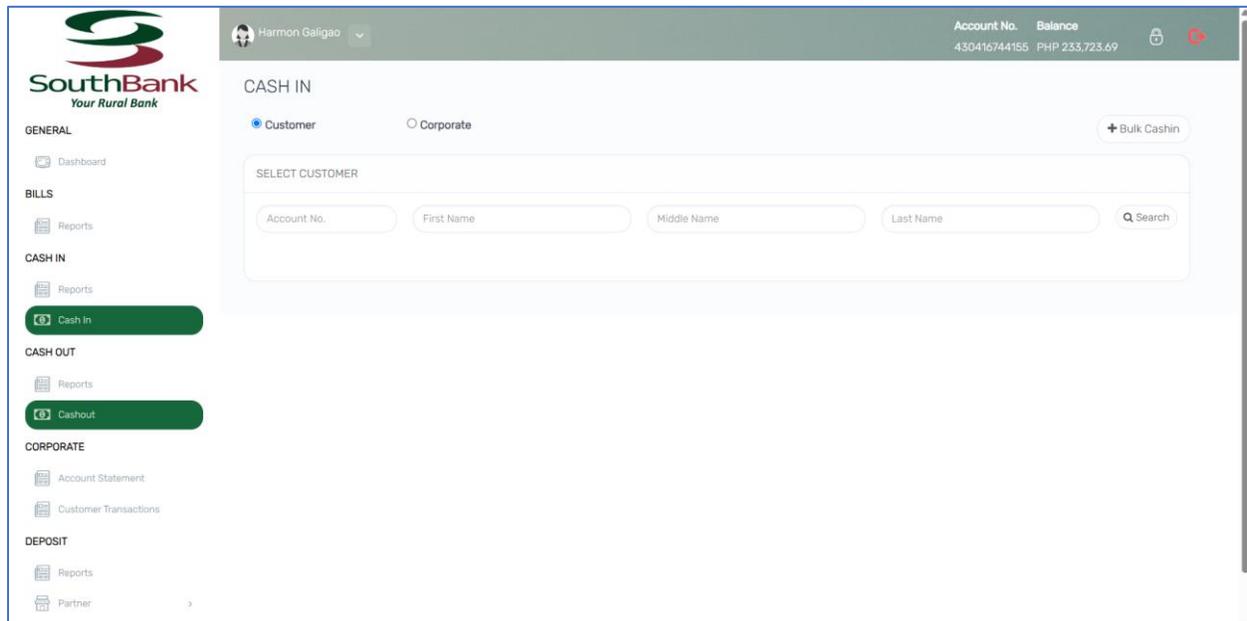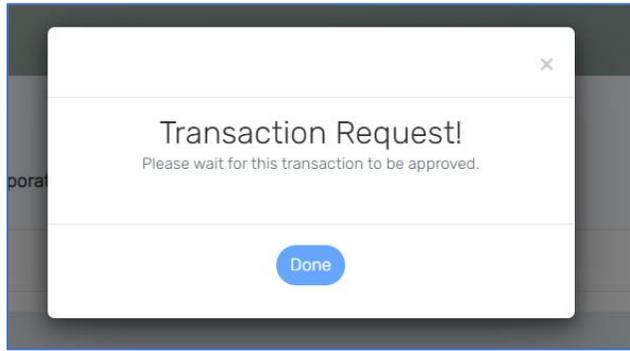

Login to your corporate account and select Cashin from the side Menu.
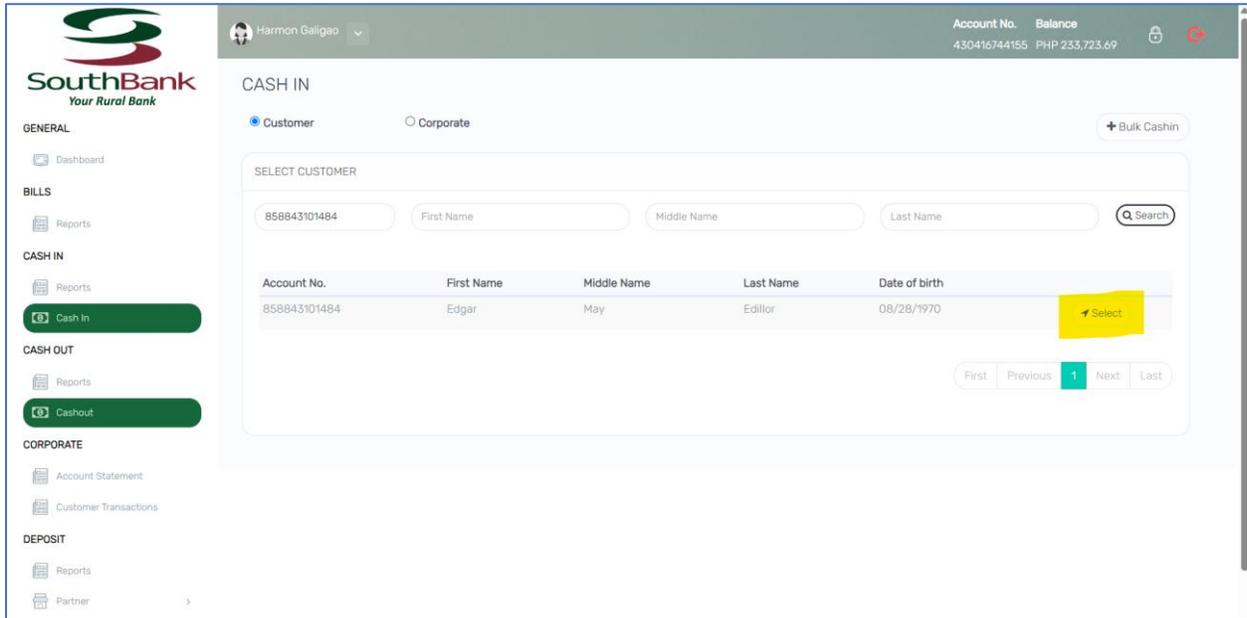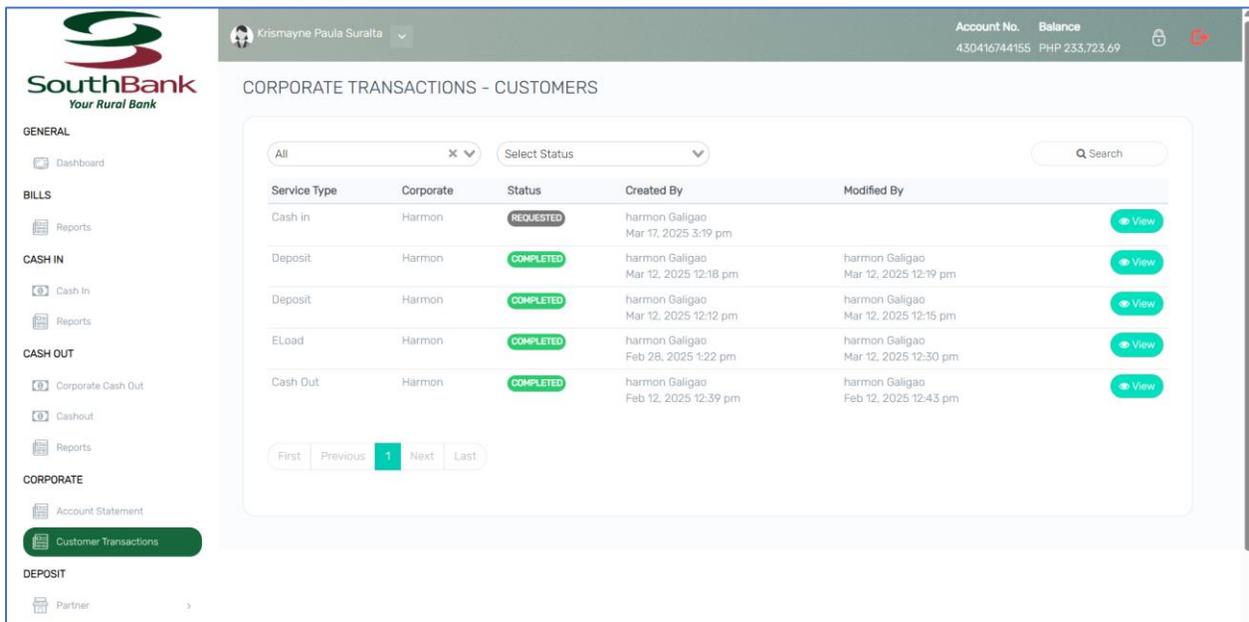

Search and select the targeted account.
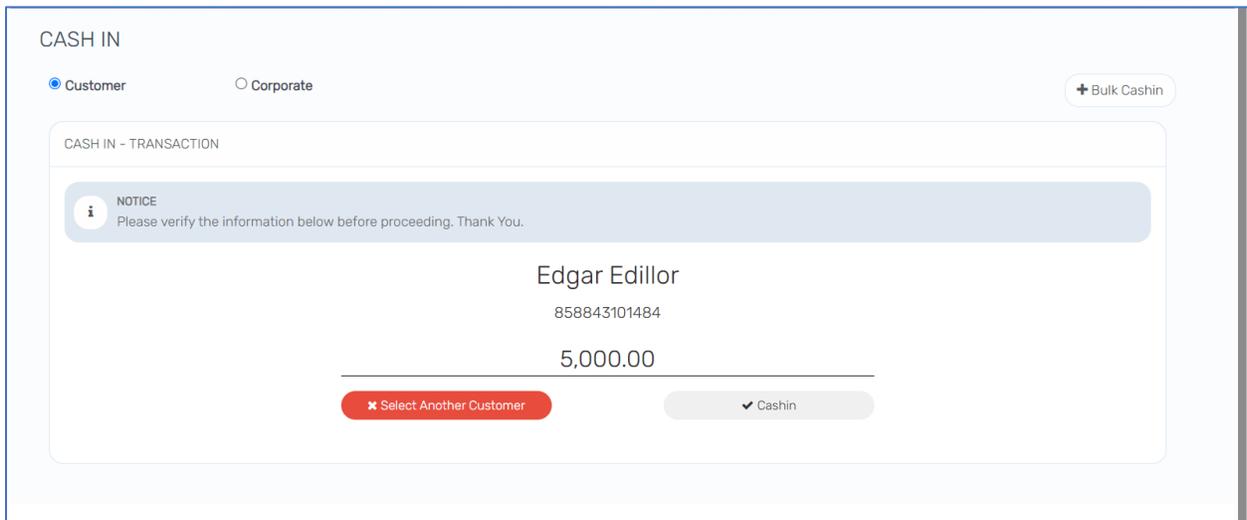
Fill in the amount to be transferred and then click Cashin

A window will pop up confirming the request.

From the Corporate Approval Account, Select Customer Transactions Under Corporate Men, then select the targeted request.

Corporate Transaction

Transaction ID

3367793

UUID

795a7750-15be-4a4b-9370-afc5f45a6b33

Request

```
        "branchName": "UAT-BRANCH",
        "prefix": "UATBRANCH001"
      }
    }
  ],
  "isMember": "1",
  "userForVerify": null
},
"request": [
  {
    "name": "_token",
    "value": "J4XCm8JhFUZ87ieE1pDjUd5WfuhYmJCz3l
ijD5TW"
  },
  {
    "name": "accountNo",
    "value": "858843101484"
  },
  {
    "name": "amount",
    "value": "5000"
  }
]
}
```

Status

REQUESTED

Service Type

Cash in

Remarks

Requested by

harmon Galigao

Mar 17, 2025 3:19 pm

Modified by

Confirm Password

Confirm Password.

Approve   Reject

Requests can be either be approved or Rejected. If approved, then confirm your password and then select Approve.

3. BANK TRANSFER

This facility enables seamless interbank fund transfers using InstaPay or PESONet channels. It is particularly useful for businesses that need to transfer funds from a SouthBank account to other bank accounts efficiently and securely.
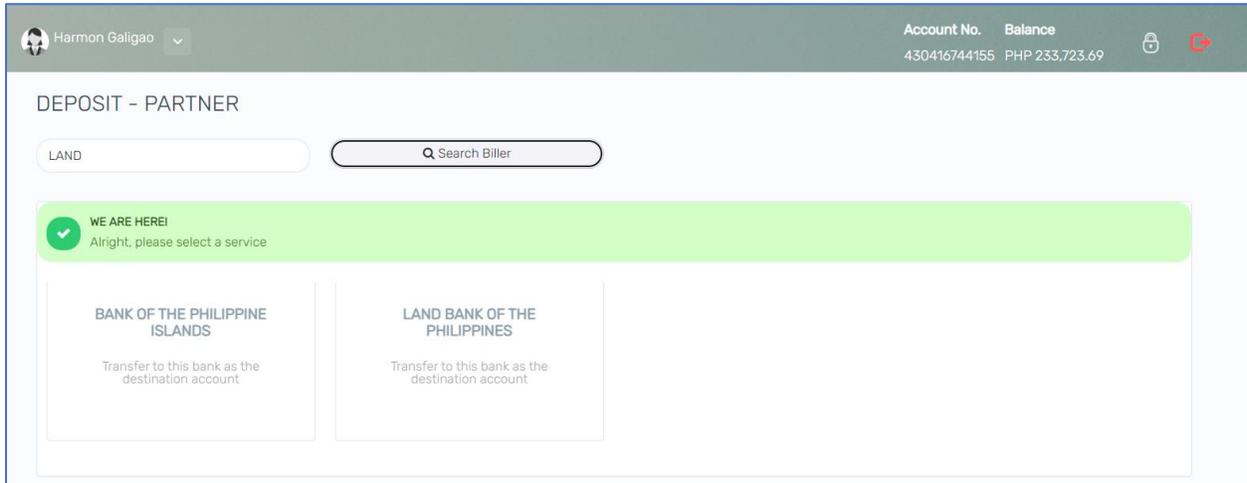
Process Flow:

- **Transaction Initiation:** The transaction maker initiates the bank transfer via the Business Account Portal. A transaction request form must be accurately filled out, including the recipient's bank account details and other required information. Once submitted, the request is forwarded for the approver's review.

- **Approval Procedure:** The approver reviews the request using the designated approval tool. To authorize the transaction, the approver must input a password and a one-time password (OTP) for verification.

- **Transaction Fulfillment:** Upon approval, the transaction appears in the maker's account via the Customer Transaction Module, where it must be confirmed before final processing.

- **Notifications:** Automated notifications are sent at each stage of the process—to the maker and approver—ensuring transparency, security, and timely updates on transaction status.
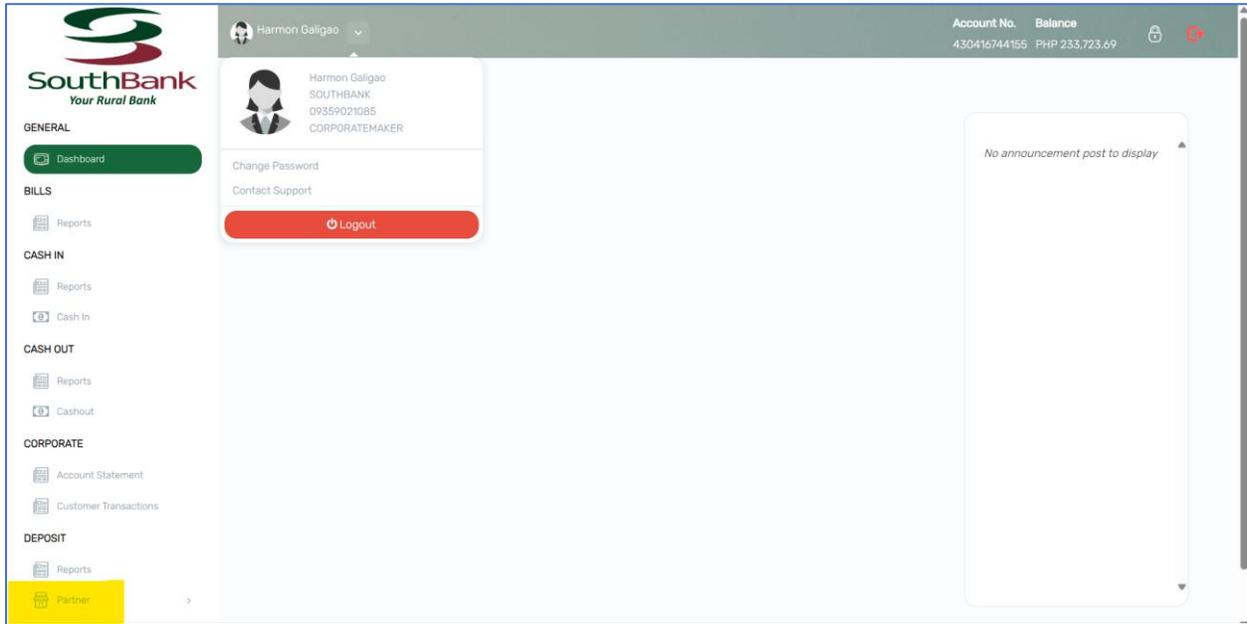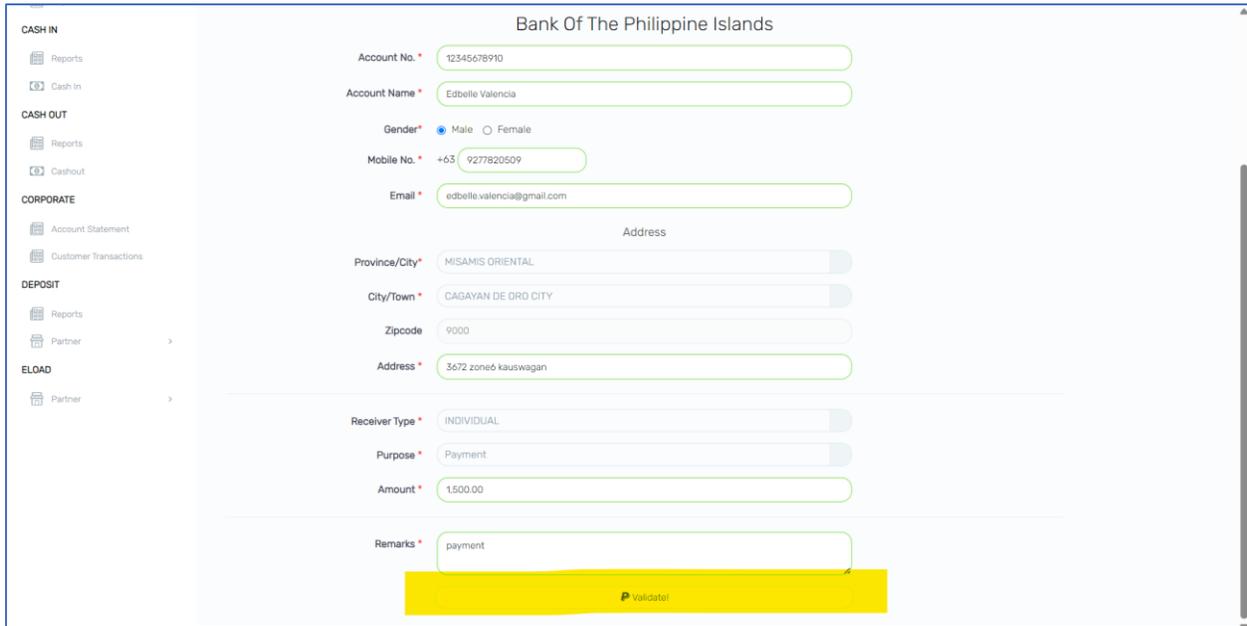
Login to your Corporate account and select Partner under Deposit Menu
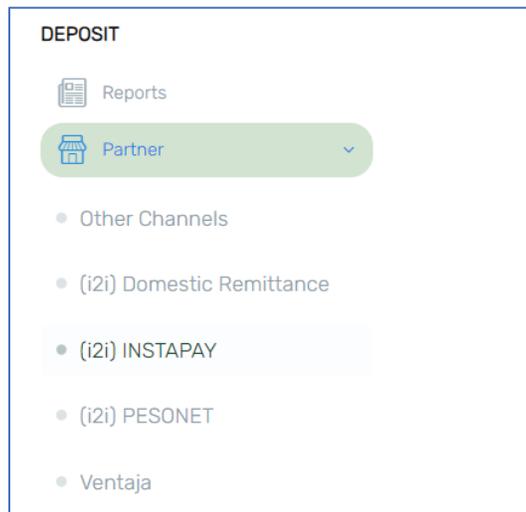
Under Partner, select either INSTAPAY or PESONET

To search, type in the recipient Bank and then select the targeted Bank from the results

Fill in the necessary details and then select Validate

4. BILLS PAYMENT

This facility enables Business Accounts to facilitate bills payments to a wide array of direct billers or through partner biller networks. It is especially beneficial for businesses with recurring or bulk obligations, ensuring a convenient and systematic approach to managing outgoing payments.

Process Flow:

• Transaction Initiation

The transaction maker initiates the bills payment transaction via the Business Account Portal**.** The required transaction form must be accurately filled out with complete biller details and payment information. Once submitted, the request is automatically routed to the designated approver.

• Approval Procedure

The approver accesses the request using the designated Approval Tool**.** To validate and authorize the transaction, the approver must input their account password and a One-Time Password (OTP) as part of the multi-factor authentication process.

• Transaction Processing

Upon successful approval, the transaction becomes visible in the maker's account through the Customer Transaction Module**.** The maker must confirm the transaction in this module to complete and execute the payment.

• Notifications

Automated system notifications are dispatched at each step of the transaction process to both the maker and the approver. These alerts provide real-time updates and promote transparency, accountability, and security throughout the transaction lifecycle.

• Fees

Applicable transaction fees are automatically computed and displayed based on pre-configured criteria. These may vary depending on the selected biller or bills payment option (direct or partners).
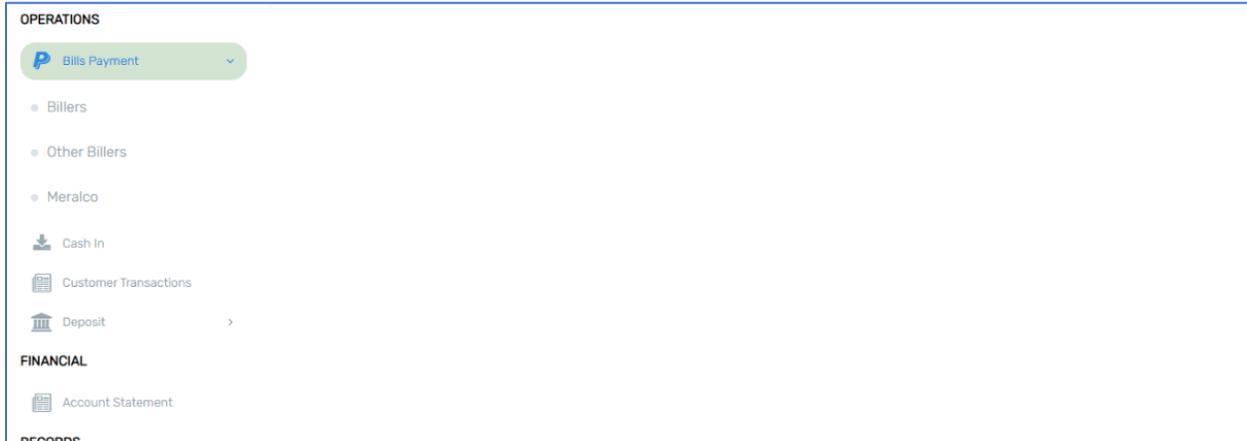
Using this interface enables you to access the bill payment facility.
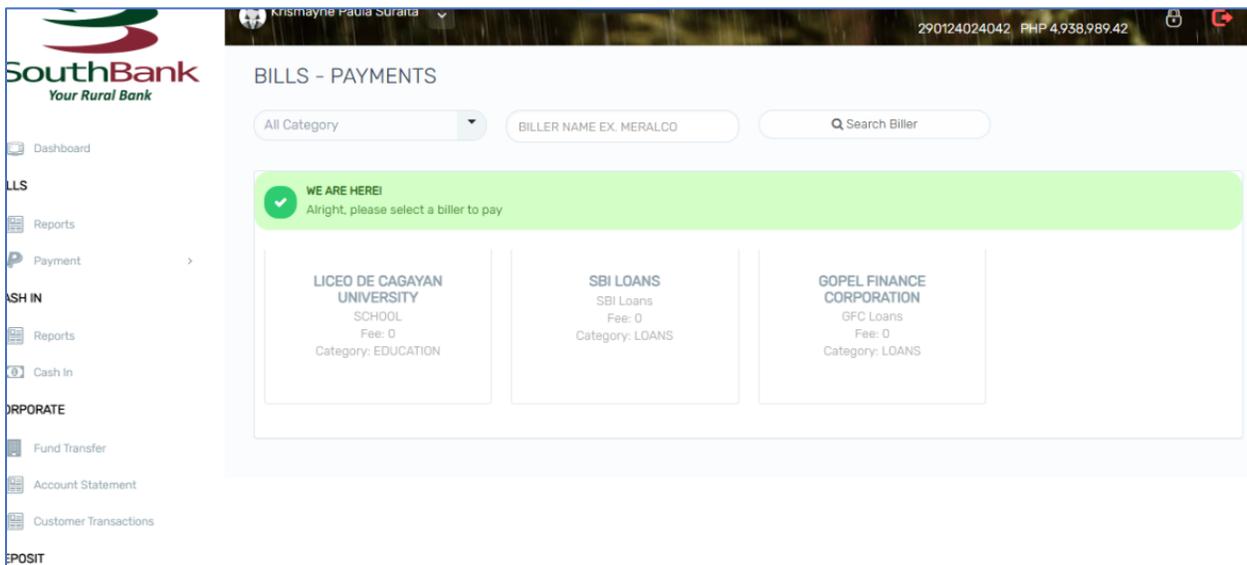
Displays the biller network of the bank.

On this interface, input the necessary details of the transaction. After the transaction, a confirmation/validation receipt is generated.

8.0 Financial Operations

The Financial Operations feature provides branches and the head office with tools to view reports, manage financial activities, and process requests. These functions ensure streamlined financial operations and comprehensive oversight.

Features and Functions:

1. Fund Request

A centralized tool for initiating and processing fund transfers between branches and the head office.

Key Capabilities:

- Structured submission and approval workflows.
- Real-time status tracking (e.g., approved, pending, rejected).
- Access to detailed fund request reports including historical transactions.
- Support for attachments and supporting documents during submission.

2. Account Statement Viewer

Allows authorized users to generate detailed transaction reports conducted via SBPay.
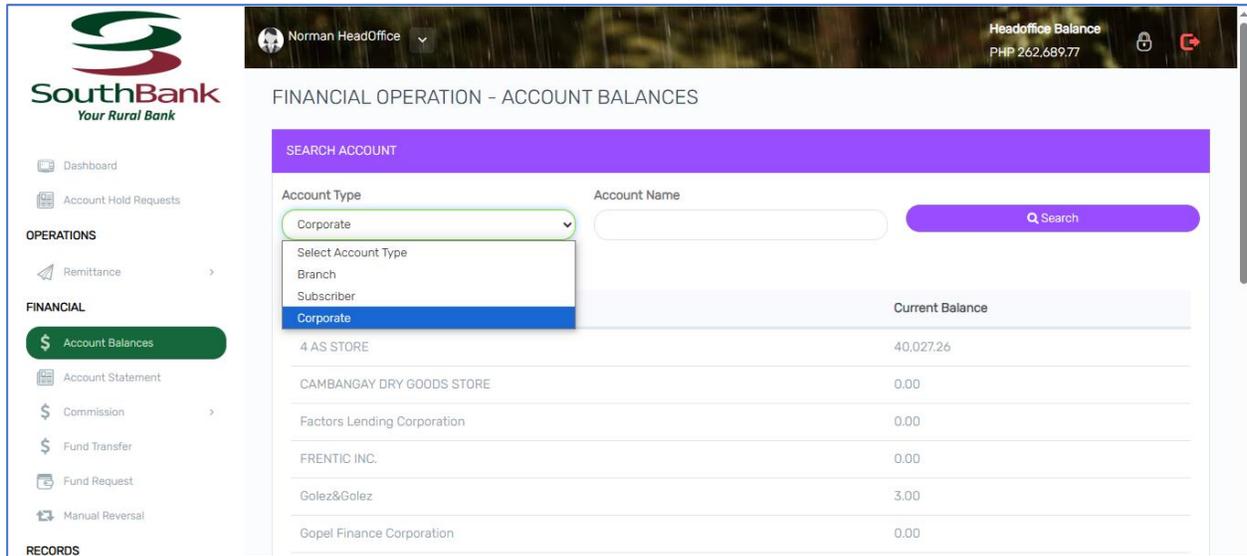
Features:
- Filter by date range for targeted reporting.
- Categorize by transaction type (e.g., branch-level, individual, or business).
- Exportable reports in Excel or PDF formats for documentation or audit use.

3. Account Balance Monitoring

Provides an overview of current balances across all relevant accounts, enabling effective financial decision-making.

Includes:
- Real-time viewing of:
    a) Branch accounts
    b) Individual customer accounts
    c) Business (OBB) accounts
- Consolidated and account-specific views for operational transparency.

THE INFORMATION IN THIS DOCUMENT MAY NOT BE DISCLOSED WITHOUT THE PRIOR WRITTEN
CONSENT OF SOUTHBANK INC. | PRIVATE AND CONFIDENTIAL

Page | 57

This module enables you to see account balances either from the Branch, OBB Account (Corporate), or the specific individual account.

Using this interface, the account statement holds various transactions recorded either from a specific branch, an OBB account, or an individual account. This can be extracted via a date range and can be generated using a PDF or EXCEL format.
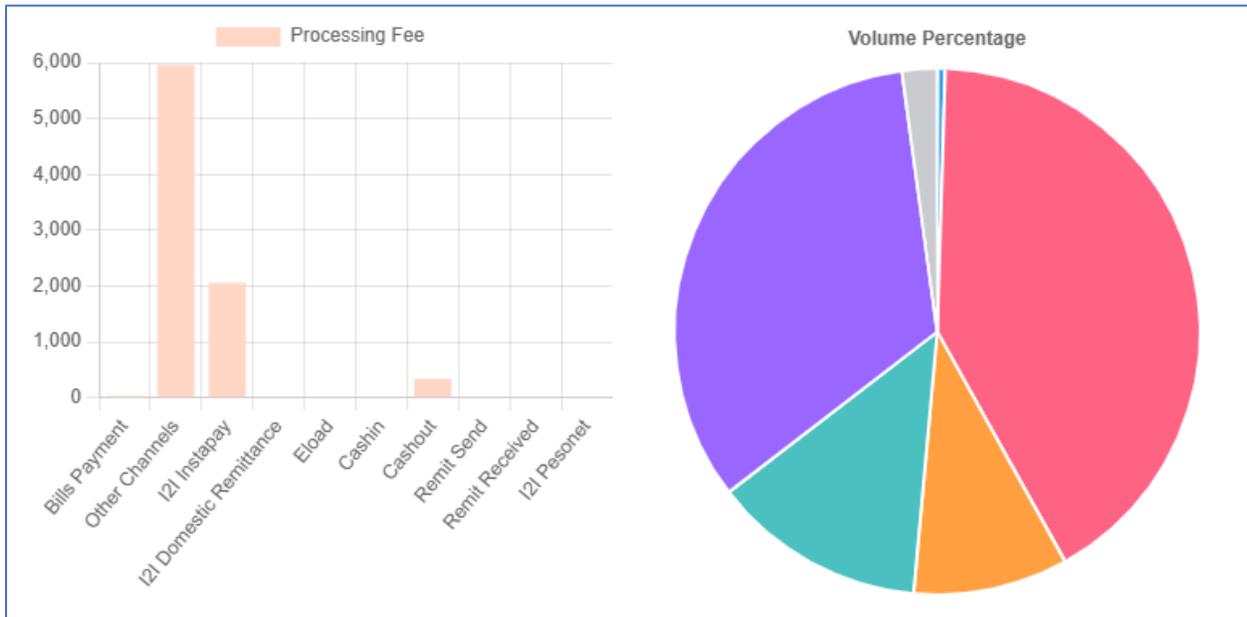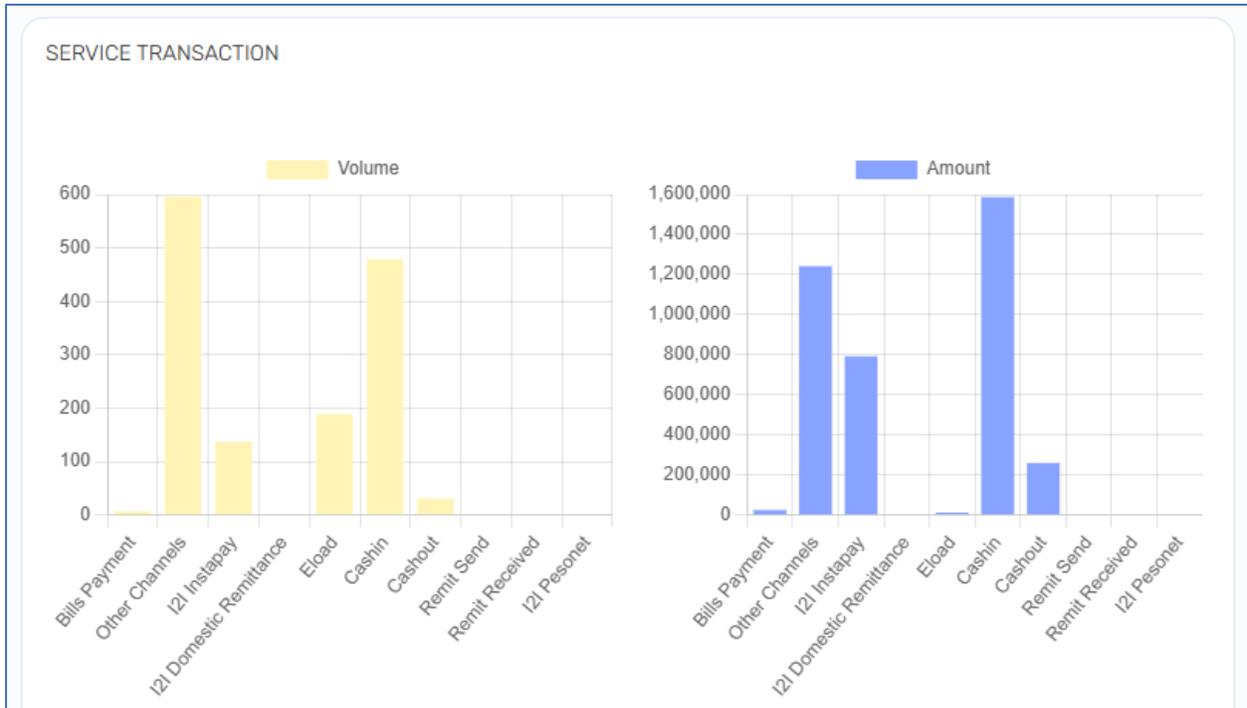
Graphical reporting based on the transactions.

9. Special Functions and Support Tools

These tools are integrated into the system by default to support operational troubleshooting, handle client support inquiries, and enforce validation and control measures. They play a critical role in addressing issues proactively and mitigating potential risks. This feature ensures operational control and minimizes risks associated with transactional errors or discrepancies, contributing to smooth and secure banking operations.

9.1 Account Hold Request

This tool allows branch offices to request a hold on a client's account balance. It is a control mechanism designed to address scenarios that require client-side clarification, including:

- Troubleshooting account discrepancies.
- Incorrect account details during cash-in or deposit.
- Errors in fund recipient information.
- Facilitating Digital Loan Management System integrations, particularly during loan disbursement.

Procedure:

1. Initiate Request at Branch Level:

- The branch logs into the system and navigates to: **General Dashboard > Account Hold Request.**
- In the request menu:
  - Input the account name or account number of the target account.
  - Specify the amount to be held.
  - Set the duration for the hold and select the auto-renew option, if applicable.
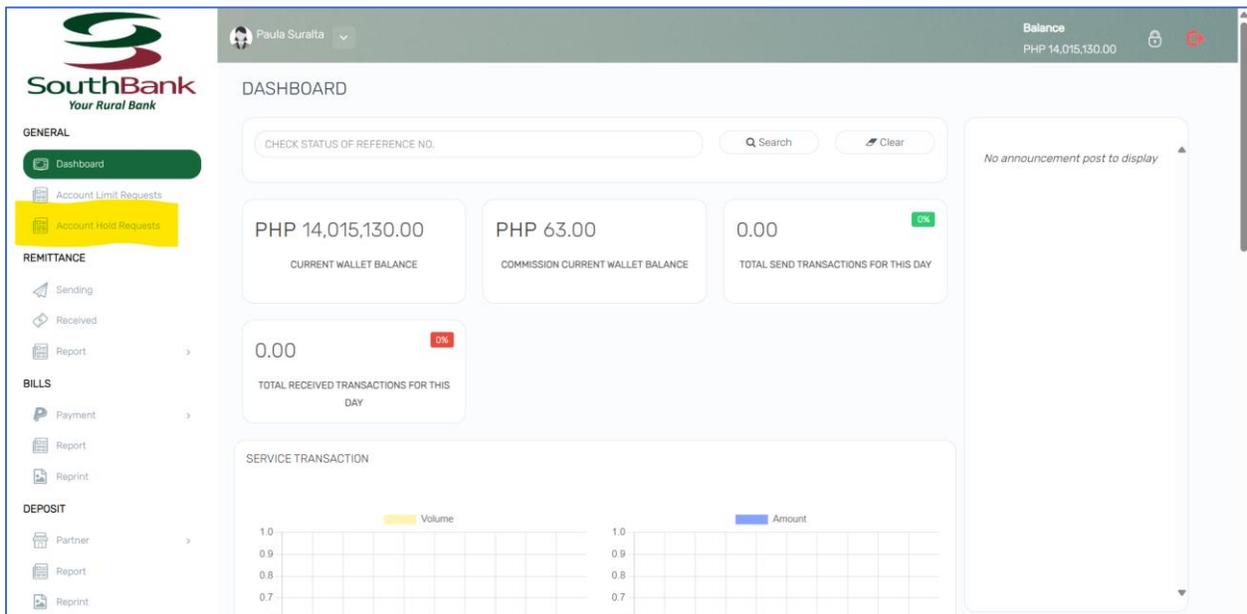
From the Dashboard, select Account Hold Requests.
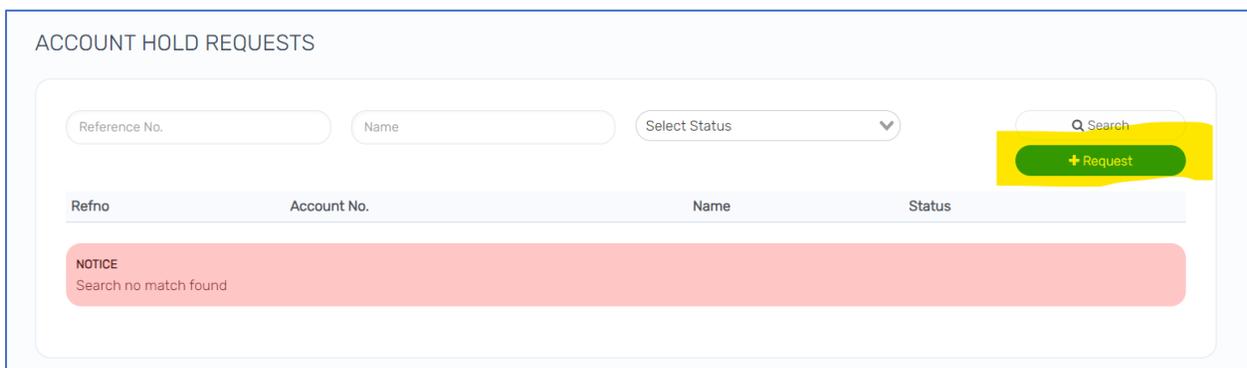
Click the Request button.

Search for your targeted account and click the Edit icon.

Input the necessary details and then click the Save icon.

THE INFORMATION IN THIS DOCUMENT MAY NOT BE DISCLOSED WITHOUT THE PRIOR WRITTEN
CONSENT OF SOUTHBANK INC. | PRIVATE AND CONFIDENTIAL

Page | 62

2. Request Submission:
- Save the request in the system.

3. Head Office Decision:
- The request will be transmitted to the Head Office for evaluation and approval.
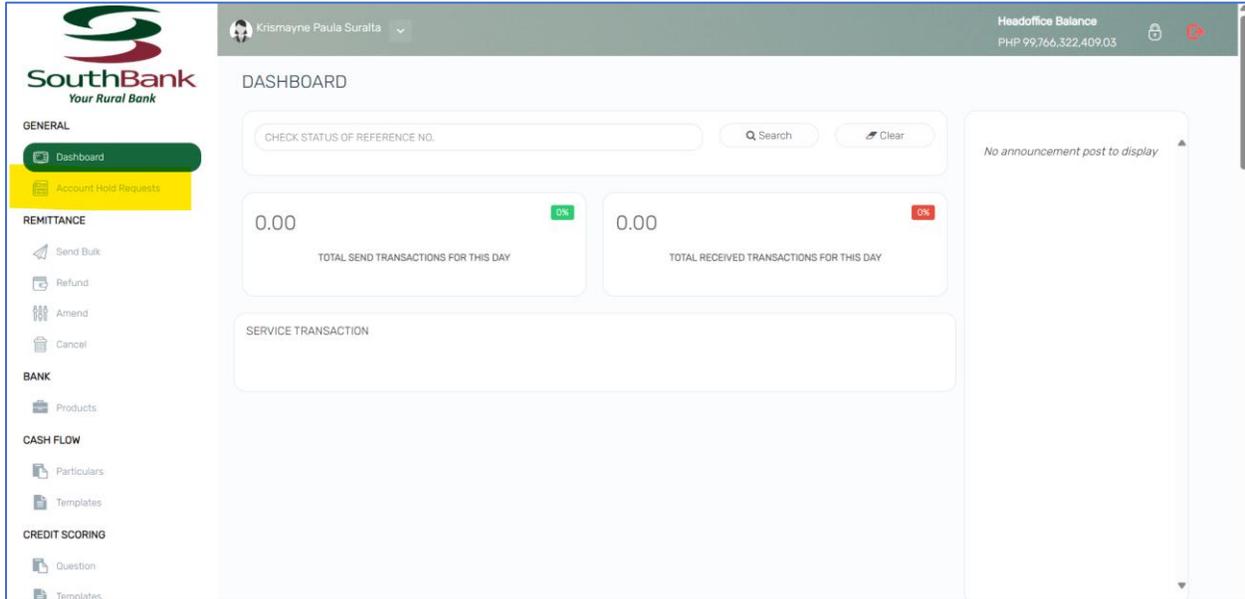
On the Approver side (HO) select Account Hold Request
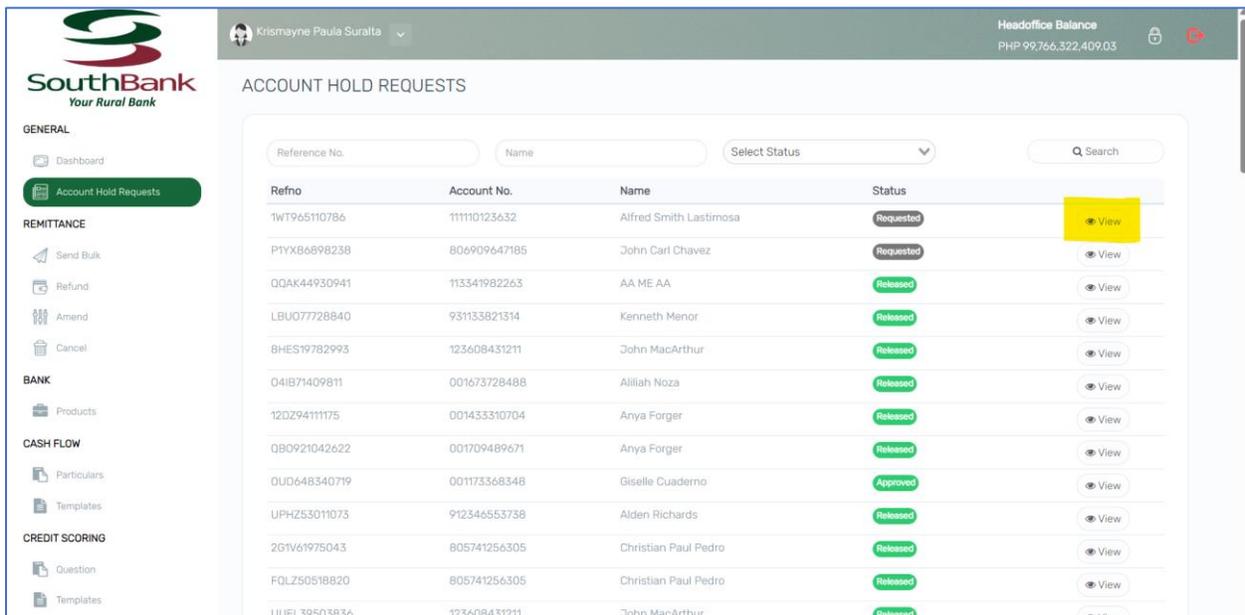
View the targeted Request
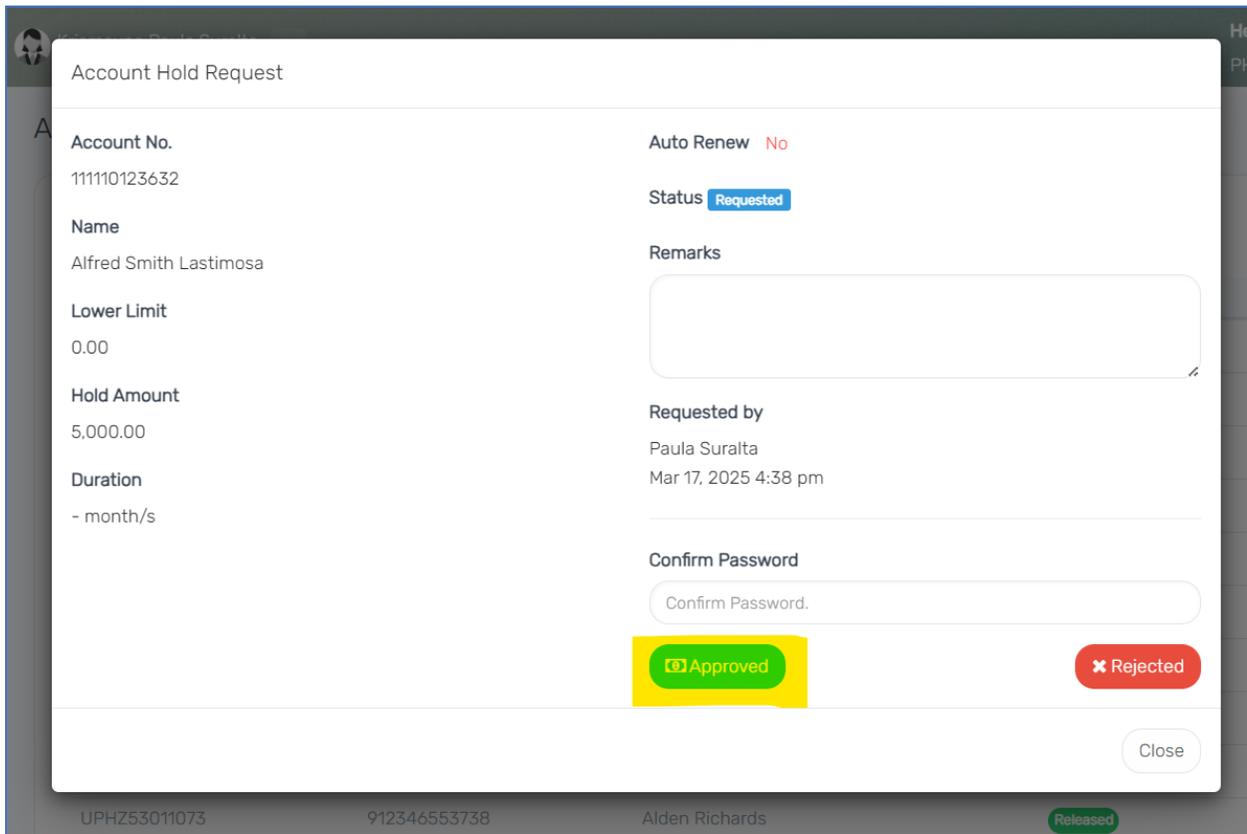
To Approve, type in your password and then click Approved

4. Post-Approval:

- Upon approval, the system will enforce the hold as specified.
- Notifications regarding the hold status will be sent to the concerned branch and client.

9.2 Account Deactivation

Purpose:

This feature empowers the Bank to implement security controls over customer accounts when risks or irregularities are reported or detected. It ensures proactive measures can be taken to safeguard financial assets and maintain system integrity.

Triggers for Account Deactivation

- **Reports Initiated By:**

  o **Client**: Requests account deactivation due to suspected compromise or misuse.
  o **Branch**: Reports irregularities or requests deactivation as a precautionary measure.
  o **Head Office Support**: Identifies risks through monitoring or investigation.

- **Supporting Documentation:**

  o All deactivation requests must be accompanied by a formal report, either submitted via the support ticketing system or based on findings from a detailed investigation or RCA.

Deactivation Procedure

1. **Login and Access:**
   o The Head Office user logs into the system.
   o Navigate to: **Registration > KYC > Profile.**

2. **Identify the Target Account:**
   o Search for the account using one of the following:
     - **Account Number**
     - **Full Name**
     - **Customer Number**

3. **Initiate Deactivation:**
   o View the profile of the targeted account.
   o Scroll to the bottom section and select the **"Deactivate Account"** option.
   o The system will prompt for confirmation before proceeding.

4. **Effect of Deactivation:**
   o Once deactivated, the account is immediately disabled, preventing the user from accessing the system.

- If the deactivated user attempts to log in, an **in-app notification** will notify them of the account status.

Reactivation Procedure

1. **Conditions for Reactivation:**
   - Reactivation is allowed only after the issue or concern has been resolved satisfactorily.

2. **Process:**
   - Follow the same navigation and input procedure.
   - Select the **"Reactivate Account"** option.
   - Log the resolution and reactivation details in the task workflow management system.
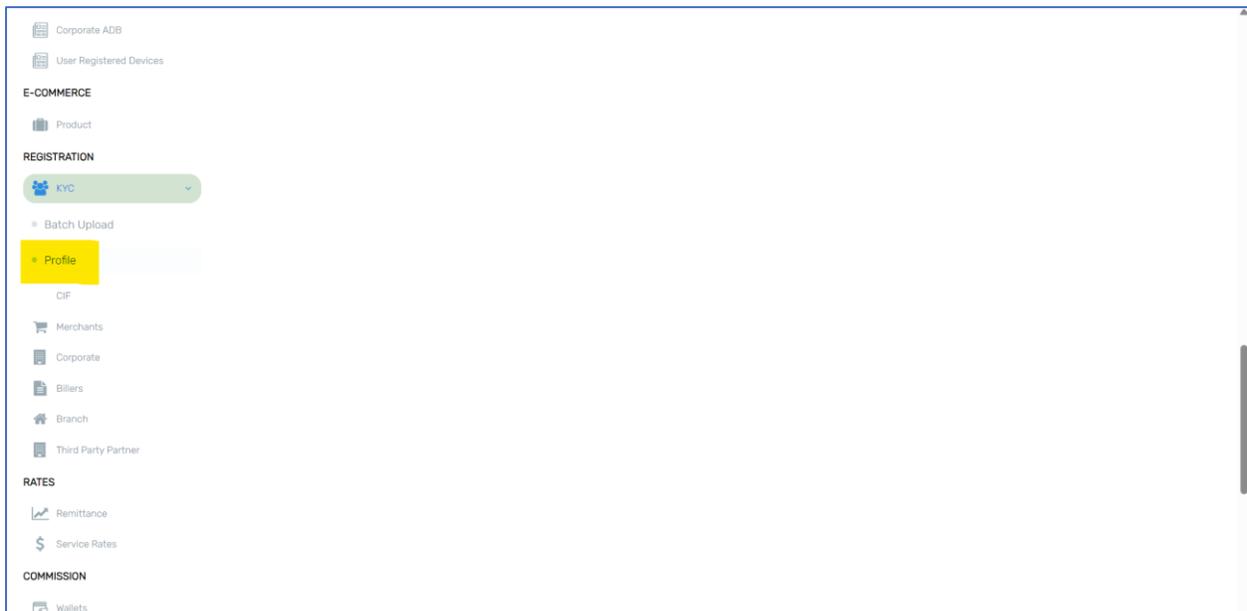
Select Profile Under Registration>KYC on the side menu
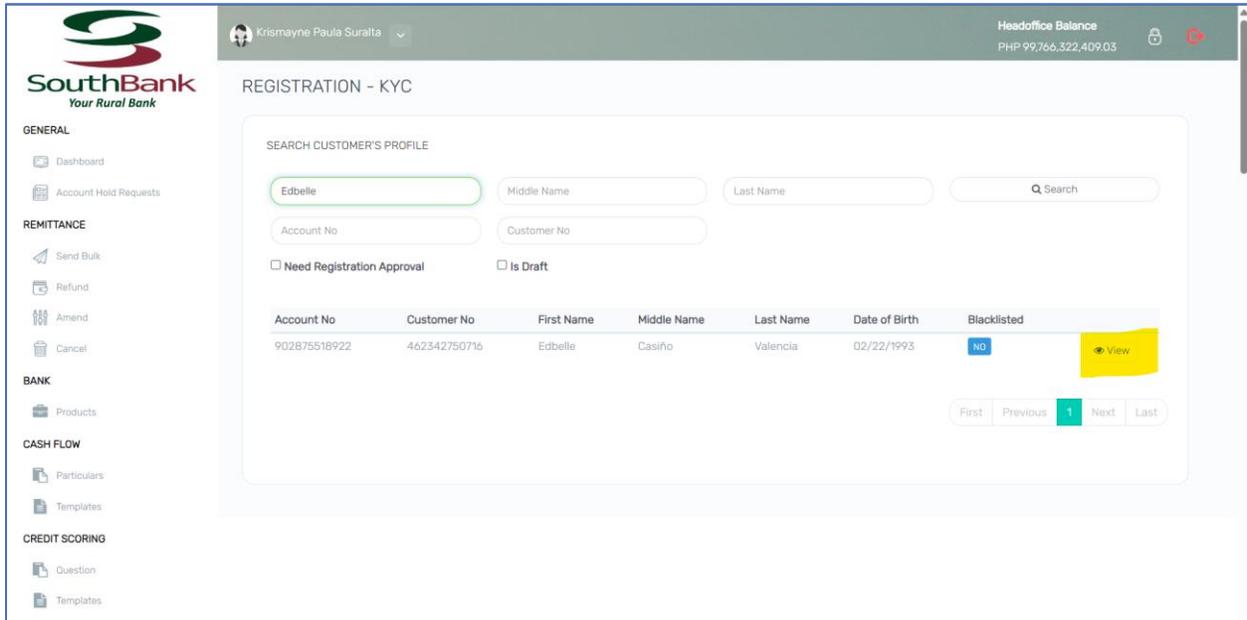
Search for your targeted account and click view
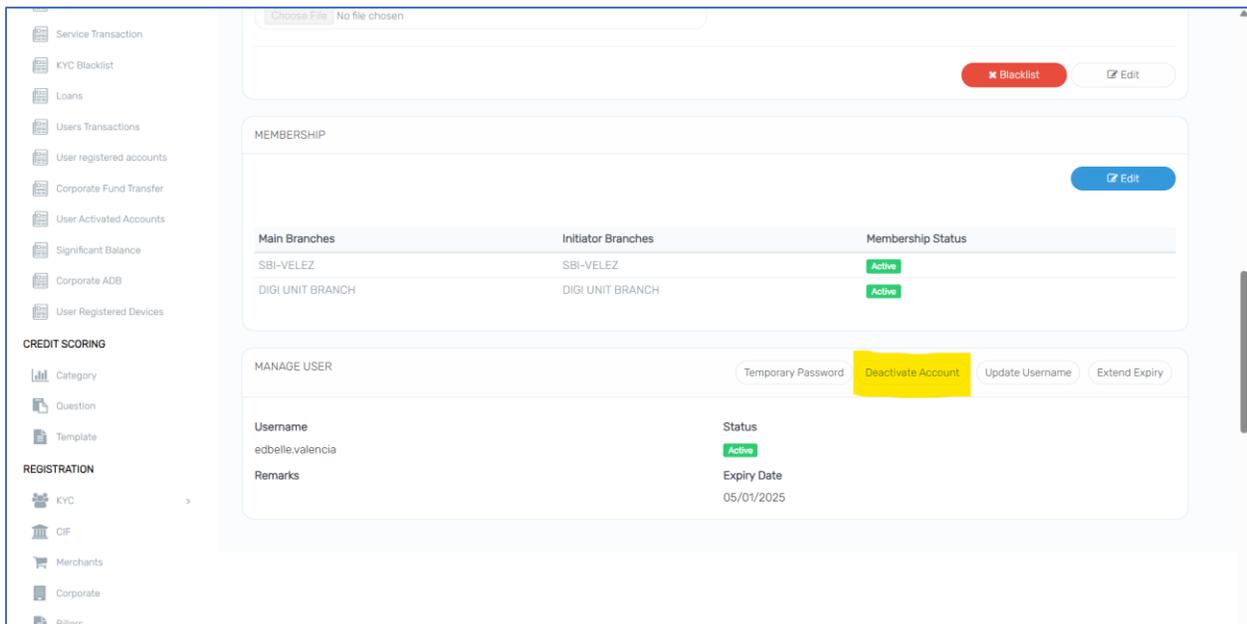
Below, Select Deactivate Account
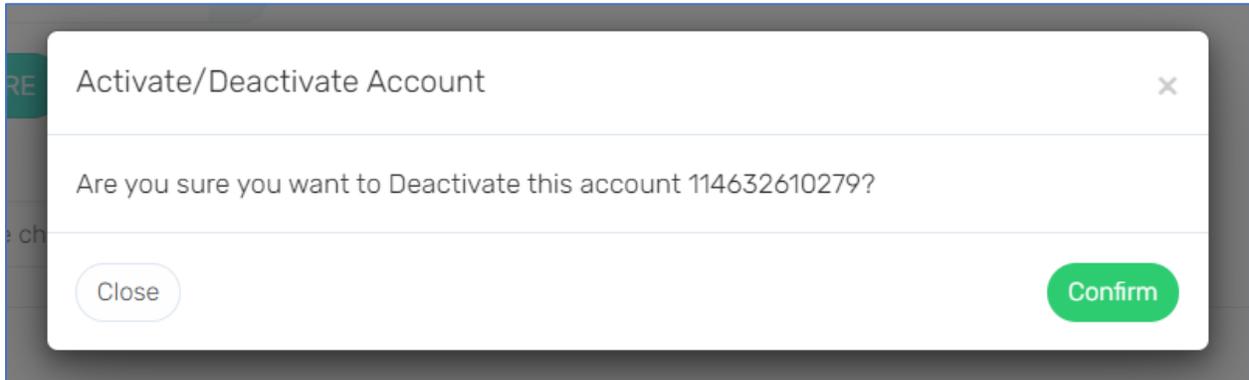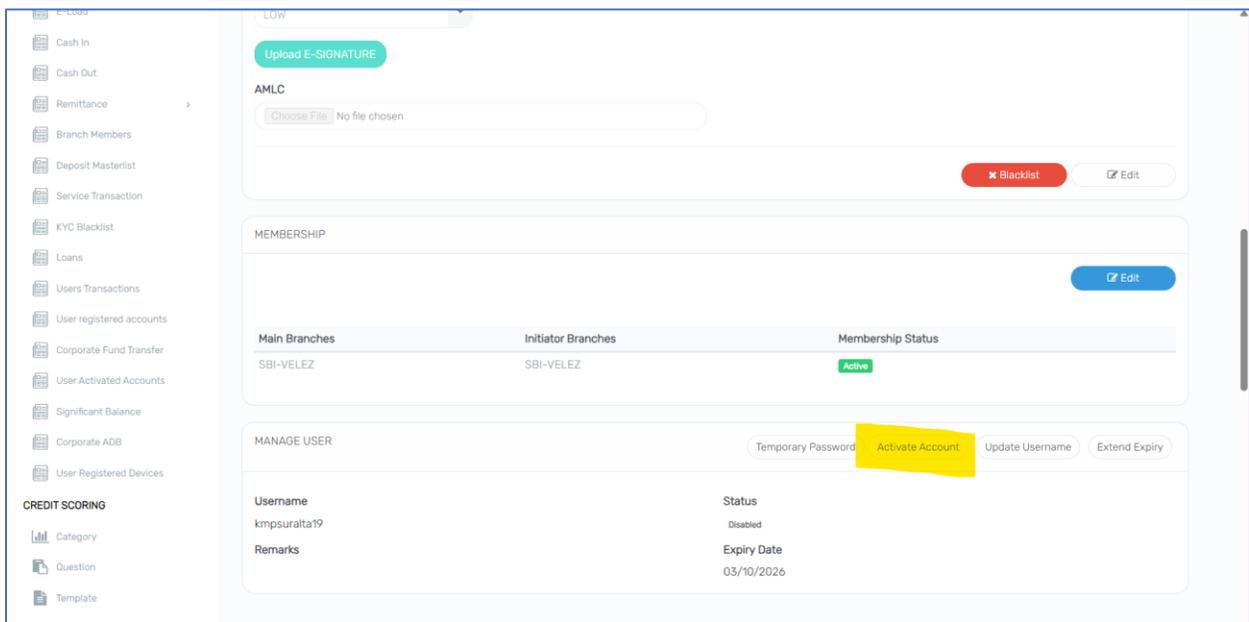
Click Confirm

To Reactivate, Select Activate Account
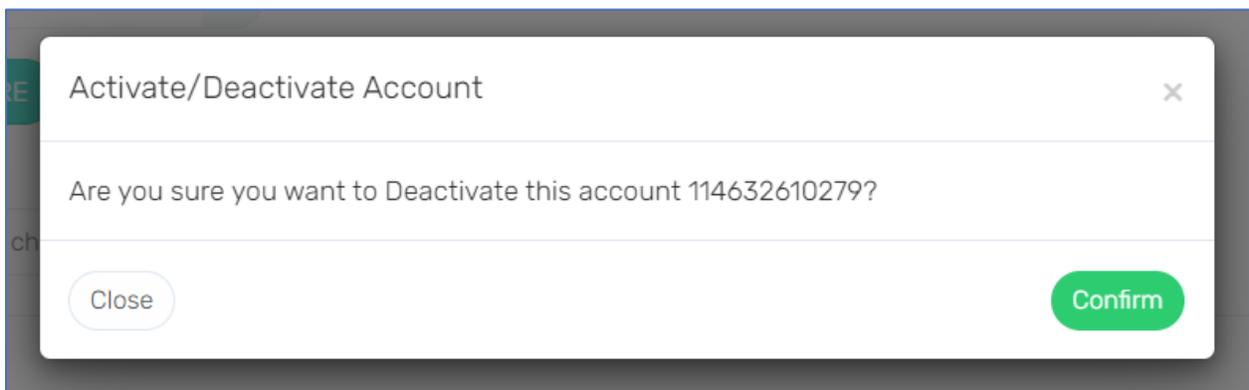
Click Confirm to reactivate

9.4 Manual Reversal

Purpose:

The Manual Reversal tool is designed to reconcile transaction-related issues, allowing the bank to issue system-based refunds for all confirmed failed transactions under SBPay. It ensures accountability, transparency, and seamless handling of transactional discrepancies.

Key Benefits:

- Ensures transparency and accountability in handling failed transactions.
- Provides a structured approach to reconcile transactional discrepancies.
- Minimizes client inconvenience through timely resolution and notification.

Process Overview:

1. **Debiting Rule:**

   - The system follows a **"debit-first" rule**, meaning the client is debited during the initiation of a transaction, whether it succeeds or fails.
   - For every transaction, the client receives a notification with the transaction status.

2. **Client Action:**

   - The client must submit a **support ticket** through the designated support channels, providing the following details:
     - Transaction Reference Number
     - Transaction Date
     - Type of Service (e.g., eccash, bank transfer, etc.)
     - Other pertinent details

3. **Initial Validation:**

   - The support ticket is received by Level 1 Support at the Head Office.
   - A task workflow is created for monitoring and tracking.

4. **Transaction Confirmation:**

   - The transaction is validated to confirm failure and legitimacy for reversal.
   - This includes access to report confirmation from partner portals (ecpay,i2i) to confirm the transaction status.

5. **RESOLUTION ISSUANCE:**

Steps to Perform Manual Reversal:

- **MAKER / INITIATOR**

1. **Login to the System:**

   - Navigate to **Financial Operations > Manual Reversal**.

2. **Enter Transaction Details:**

   - Select the type of service (e.g., bills payment, fund transfer).
   - Input the **Transaction Reference Number**.
     (Note: The process cannot proceed without the reference number.)

3. **Confirm and Authenticate:**

   - Authenticate the process by entering the password of the user performing the reversal.

4. **Sent for approval**

   - The request will be forwarded to the designated approving authority or personnel for the necessary approval process. A system-based approval tool, available under the Head Office role, is in place to facilitate this action. Additionally, a notification will be automatically sent to the assigned approver, providing a copy of the reversal request for review and decision.

5. **Reversal Execution:**

   - Once authenticated and approved, the system automatically reverses the transaction.
   - The reversal is logged in the **Statement of Account (SOA)** for both the client and the originating branch.

For additional information, refer to **Attachment #1, Technical and Operational Support Procedure.**

- **APPROVER**

1. **Log in to the System and navigate to:**

   Financial Operations > Manual Reversal > Requests.
   Alternatively, you may click the direct link provided in the system-generated email notification.

2. Open the Request by **clicking "View" to review** the transaction details.

3. **Approve the Request** by entering your system password to confirm authorization.

4. **Completion of Reversal** – Once approved, the transaction will be automatically reversed. The adjustment will be reflected in the Statement of Account (SOA) and corresponding reports.

Post-Reversal Process:

1. **Reporting and Monitoring:**
   - Details of the reversed transaction, including date, amount, reference number, and service type, are logged in a report.
   - This report is reviewed and validated weekly by the **Bank Operations Manager**.

2. **Client Notification:**
   - The client is notified of the successful reversal through the appropriate communication channels.
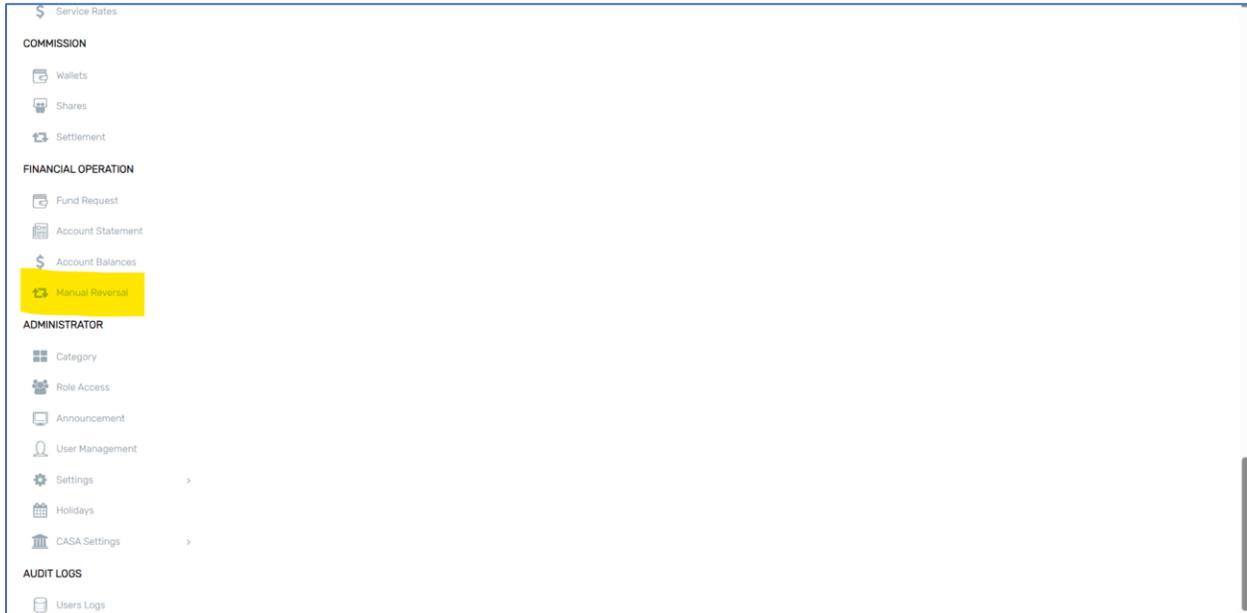
Select Manual Reversal under Financial Operation on the side menu
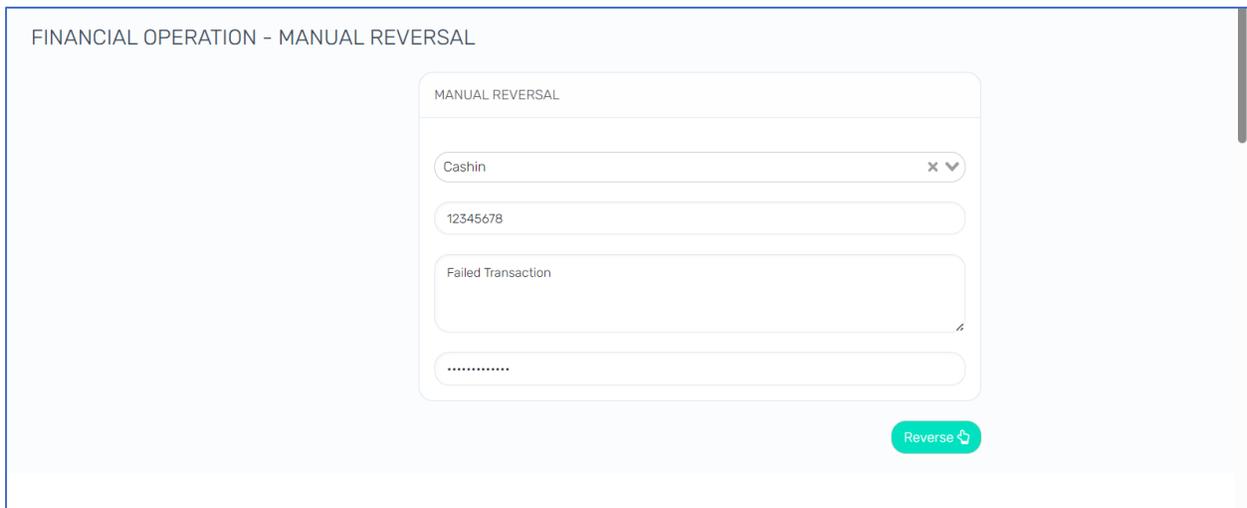
Enter the necessary details and click Reverse

10. **Operations Management and Oversight**

10.1 Training and Development

Effective training and development initiatives are crucial for the successful operation of SBPay, ensuring staff competence, enhanced security awareness, and user satisfaction. The following elements outline the structured approach for both internal employee training and external user education.

- **Employee Training Programs**

Purpose:

To equip staff with the necessary skills, knowledge, and tools to operate SBPay systems effectively while adhering to security and operational standards.

Key Initiatives:

1. **Induction Training for New Employees:**

   - Comprehensive onboarding program covering SBPay operations, security protocols, and customer service standards.
   - Introduction to system functionalities, compliance requirements (such as BSP, AMLA), and troubleshooting procedures.

2. **Role-Specific Training:**

   - Customized training for key roles, such as system administrators, finance personnel, and branch officers.
   - Specialized modules for operations like fund management, transaction reversals, and account security management.
   - Enablement through online educational tool such as SBI Academy Online.

3. **Regular Security Awareness Workshops:**

   - Focused sessions on identifying and mitigating cybersecurity threats (such as phishing, social engineering).
   - Updates on compliance and regulatory changes to ensure adherence to evolving industry standards.

4. **System Updates and Process Changes Training:**

   - Regular sessions to familiarize staff with new features, updates, or process improvements within the SBPay system.
   - Simulation exercises to practice implementing changes before real-time execution.

5. **Performance Assessment and Feedback:**

- Periodic evaluations to assess employee competency and identify areas for improvement.
- Feedback sessions to discuss challenges and opportunities for professional growth.

6. **Targeted Programs for Auxiliary Products and Services for Business/Corporate Users:**

- Training sessions for businesses on features like payroll disbursement, fund management, and account monitoring.
- Guidance on integration with other financial tools and compliance requirements specific to corporate accounts.

7. **Real-Time Support and Knowledge Base:**

- 24/7 support channels to address user queries and resolve issues promptly.
- A comprehensive knowledge base with searchable articles on common topics and troubleshooting steps.

Expected Outcomes:

- Enhanced operational efficiency and reduced errors.
- Improved employee confidence and job satisfaction.
- Strengthened compliance and security standards.

10.2 Daily Operational Procedures

Key objectives:

- Smooth and error-free daily operations.
- Accurate transaction processing and reconciliation with partners.
- Minimized risks associated with failed transactions or financial discrepancies.

Transaction Monitoring (Branches, Settlement, Operations and Finance):

1. Real-Time Dashboard Monitoring:

- All units and personnel involved in the process are responsible for actively monitoring transaction activities via the SBPay system dashboard. Their role is to ensure that all transactions are processed efficiently, accurately, and without delays or errors.
- Identify anomalies, such as failed or pending transactions, and escalate issues requiring immediate attention.

2. **Partner Platform Monitoring (UBX and ECPay):**

- The settlement unit and the support group ensure and processes cross-checking of transactional data between SBPay and partner systems to ensure alignment and detect discrepancies.
- Technical Group and partner system provider ensure and monitor API uptime and system performance to identify potential integration issues.

3. **Threshold Alerts and Notifications:**

- Utilize system notifications for low balances, failed transactions, or system anomalies.
- Escalate unresolved issues to technical support in both internal and third-party providers.

Reconciliation Procedures: (Branches, Settlement, Operations and Finance):

1. End-of-Day Balancing:

- All units and personnel involved in the process are responsible for generating and reviewing daily transaction reports from SBPay and/or partner systems (UBX, ECPay).
- Compare branch wallet balances and transaction records against the system's settlement reports to ensure consistency.

2. Discrepancy Resolution:

- All units and personnel involved in the process must coordinate, investigate (as needed), and document any mismatched transactions to ensure proper resolution.
- Any discrepancies should be promptly reported to the settlement unit, support group, and operations unit for resolution, accompanied by thorough documentation of the adjustments made.

3. Consolidated Reports Submission:

- Submit reconciled reports, including a summary of transactions, fund movements, and resolution logs, to the branch officer (for branches), operations unit, finance department by end-of-day cut-off.

Reversal Procedures:

1. Triggering Reversals: (Branches, Support Group, Settlement, Operations and Finance):

- Identify transactions eligible for reversal, such as duplicate charges, failed transactions with debits, or system errors.
- Confirm the legitimacy of the reversal request through supporting documentation or client communication.

2. System-Based Reversal Process:

- Use the SBPay system's Manual Reversal feature to initiate the reversal.
- Input required details, including the transaction reference number, type of transaction, and reason for reversal.

3. Verification and Approval:

- Secure approval from the operations unit before initiating the reversal process.
- This approval request should be submitted via email, including all transaction details and the necessary supplementary attachments for verification and documentation.
- Document the reversal in the system's task workflow for accountability.
- Generate a weekly report detailing all reversal transactions.
- The operations unit shall review the report to confirm and cross-check the accuracy and legitimacy of the processed reversals, ensuring compliance with internal controls and policies.

UBX and ECPay Operations:

1. **Partner-Specific Reconciliation:**

   - Use designated UBX and ECPay portals to cross-check transactions with SBPay records.
   - Address any delays or missing transactions directly with the partner's support team via email or other medium.

2. **Coordination with Partners:**

   - Maintain active communication channels with UBX and ECPay for real-time issue resolution.
   - Follow partner-specific protocols for escalations or adjustments outside SBPay's control.

3. **Audit and Reporting:**

   - Document and archive daily reports, including discrepancies and resolutions, for audit and compliance purposes.
   - Perform periodic reconciliations to ensure long-term accuracy and alignment with partner accounts.

10.3 SYSTEM ACCESS AND USER MANAGEMENT

Purpose:

To establish a structured process for requesting, granting, and terminating system access to ensure security, accountability, and compliance within SBPay's operational framework.

Key objectives:

- A streamlined and transparent system access management process.
- Improved security through controlled access and timely termination.
- Reduced risks of unauthorized access or data breaches.
- Documented accountability for all access requests and terminations.

Applicable Forms and Procedures for System Access Management:

1. **Requesting and Approving Access:**

Form: System Access Request Form (SARF)

- **Purpose:** Used for requesting access to SBPay systems, including new accounts or additional permissions for existing accounts.

- **Details Required:**

  - Employee's Full Name, Job Title, and Department
  - Specific system/module to access (such as SBPay Portal, LMS etc.)
  - Reason for access (such as job role, temporary project etc.)
  - Line Manager/Department Head approval

- **Supporting Documentation:**

  - Employment contract (for new users) or role change memo (for permission updates).

- **Approval Workflow:**

    - Verification and approval must first be obtained from the requesting department's or branch head to ensure alignment with operational needs.
    - The Operations Head shall review and approve the request to confirm its compliance with operational guidelines.
    - The Chief Technology Officer (CTO) must also verify and approve the request, ensuring it aligns with technical and strategic objectives.
    - Once all necessary approvals are obtained, the IT Support Group will execute the request and document the process for audit and tracking purposes.

3. **Terminating Access:**

- **Form: Access Termination Request Form (ATRF)**

    - **Purpose:** Used to revoke access for users due to resignation, termination, or role changes.

    - **Details Required:**

        - User's Name, Employee ID, and Department
        - System/modules to deactivate
        - Reason for termination (such as: end of employment, internal transfer)
        - Signature and Approvals from the concerned personnel.

- **Procedure:**

    - The department or HR initiates the access termination process using the ATRF.
    - The IT Group or Support Group ensures all access is disabled, including credentials and access keys.
    - System audit logs are reviewed to confirm no unauthorized activity occurred before termination.
    - Notify the requestor once the process is complete.

4. **Regular Audit and Compliance:**

- Conduct periodic reviews of active user accounts to ensure permissions align with job roles.
- Review access documents, enforce password policies, and access expiration rules.

10.4 SYSTEM MAINTENANCE

Purpose:

To ensure SBPay's operational continuity and data security during scheduled or unscheduled system maintenance while minimizing disruption to services.

Key objectives:

- Minimized disruption to SBPay services during maintenance activities.
- Enhanced operational readiness and clear communication protocols.
- Improved system performance and security through effective maintenance.

A. Maintenance Announcement:

1. **Communication of Maintenance Details:**

   - **Official Announcement:**

     a) A system maintenance notice is prepared by any personnel from the DIGI unit as mandated by the department/unit head. This shall be distributed via email, system notifications, bulletin boards, memos and other channels known to the bank.

     b) The notice includes:

        - Scheduled maintenance date and time
        - Expected duration
        - Impacted services (such as: transaction processing, report generation)
        - Alternative contact details for urgent concerns.

   - **Acknowledgment and Awareness:**

     a) All relevant departments, branches, and partners are required to acknowledge the notice.
     b) Ensure that customer-facing teams (such as: branches, support group) are briefed to handle user inquiries effectively.

2. **Client Notification:**

   - For services affecting end-users (such as mobile apps, corporate/OBB accounts):
     a) Notify clients at least 8 hours in advance (for scheduled maintenance).
     b) Use system alerts, SMS, or email communication channels to inform them.

3. **Pre-Maintenance Preparations:**

- Ensure all scheduled tasks and transactions are completed before the maintenance window begins.
- Advise branches to finalize daily reports or submit critical fund requests before the maintenance window.
- Back up all critical data and transactions to mitigate risks.

B. Standard Practice:

1. **During Maintenance:**

- **Monitoring:**

   a) The IT Group monitors the system closely to ensure maintenance activities proceed as planned.
   b) Critical changes or updates are logged for review, testing and assessment.
   c) Both IT and Support Group, in coordination with third-party providers, shall compile and document all relevant information and updates to ensure proper handling and resolution of issues.

- **Operational Alternatives:**

   a) For essential operations, implement contingency plans such as manual processing for urgent transactions or redirection to unaffected systems.
   b) Escalate unforeseen issues or delays to designated unit heads, partner SPOC (Single Point of Contact), or support teams.

2. **Post-Maintenance Procedures:**

- **Validation and Testing:**

   - Conduct system tests to verify that all modules and services function correctly.
   - Validate transaction records to ensure data consistency and integrity.
   - A list of modules, functions, or services is provided by the third-party providers and cascaded to the Support Group, highlighting priority test modules for immediate validation and resolution.

- **Reactivation:**

   - Resume operations and confirm availability of all services. This information/announcement is channeled through our communication channels.
   - Remove any system notifications or alerts regarding maintenance.

- **Incident Reporting:**

  - If issues arise during maintenance, document all details comprehensively and conduct a root cause analysis to identify the underlying problem. The findings shall be recorded in the task workflow for tracking and resolution of issues and concerns.
  - Should the issue require escalation to third-party providers, a detailed report, including all relevant findings and supporting information, shall be prepared and submitted to the respective partner for further assistance.
  - Share the findings and proposed remediation steps with the relevant key personnel of the bank and all individuals directly involved, ensuring alignment and coordinated resolution efforts.

3. **Continuous Improvement:**

   - **Review and Feedback:**

     - Conduct a post-maintenance review to assess the success of the activity.
     - Gather feedback from internal and external users to identify potential areas for improvement.
     - The results of the feedback shall be reported by the Unit Head (DIGI) to the core officers of the bank after thorough assessment by the IT and Support Group. This process aims to determine the relevance and significance of the suggested enhancements, findings, or potential threats.
     - These findings and decisions shall also be documented in the minutes of meetings after which to be filed for development and implementation processes. This shall also be encoded in the task workflow for processing and monitoring.

   - **Documentation:**

     - Update system logs, operational manuals, and user documentation with any changes made during maintenance.
     - Share an official post-maintenance report with leadership, audit, and compliance teams.

10.5 Guidelines for Generating Reports for Internal Auditing and Regulatory Compliance

Key objectives:

- Comprehensive, accurate, and timely reporting for internal and external use.
- Enhanced ability to monitor operational performance and ensure compliance.
- Strengthened trust with regulatory bodies and stakeholders through transparent practices.

1. Types of Reports Generated:

a) **Internal Auditing Reports:**

- **Transaction Reports:** Summary of all financial transactions performed within SBPay, categorized by service type, branch, and date.

- **Access Logs:** Logs detailing system access, including login attempts, user activities, and changes to user roles or permissions.

- **Exception Reports:** Flagged or unusual transactions, including failed, reversed, or high-value transactions.

- **Fund Management Reports:** Fund requests, allocations, and balance summaries across all branch wallets and accounts.

b) **Regulatory Compliance Reports:**

- **AML Compliance Reports:** Customer transaction thresholds, flagged activities, and suspicious activity reports (SAR).

- **KYC Reports:** Summary of account holder verification and documentation records.

- **Settlement Reports:** Daily and monthly settlement records, including fund transfers to partner accounts (such as: ECPay, UBX).

- **Incident Reports:** Documentation of operational interruptions or security incidents with remediation details.

2. Reporting Frequency:

Depending on the agreed frequency of reporting, the following options are designed for availability.

- **Daily Reports:**
  - Transaction summaries
  - Fund balances and wallet thresholds
- **Weekly Reports:**
  - Reconciliation reports for financial operations and settlement balances
  - Issues and concerns, remedies, and resolution.
- **Monthly Reports:**
  - Detailed SOA for regulatory submissions
  - Summary of flagged transactions and exception handling.
- **As Requested Reports:**
  - As requested by auditors, regulatory bodies, or senior management.

3. Report Generation Process:

a) **Accessing the System:**

- Authorized users log in to the system with appropriate credentials.
- Navigate to the "Reports" section in the dashboard.

b) **Selecting Report Type and Filters:**

- Choose the desired report template (e.g., Transaction Summary).
- Input necessary filters, such as date range, account type, or branch.

c) **Exporting Reports:**

- Select the preferred format (e.g., PDF, Excel).
- Review the report for accuracy and completeness.

d) **Approval and Distribution:**

- Submit the generated report to the designated direct participants (such as: Bank Operations Manager, Compliance Officer, Audit, Technology Officer, Finance).

4. Internal Auditing Best Practices:

- Ensure all system logs and financial records are securely retained for the mandated period of 3 years. After this period, the reports shall be archived systematically for future reference and use.
- Regularly validate the integrity of reports by cross-referencing them with source data, either by directly accessing the system or obtaining the required information from responsible personnel.
- Utilize the feature available under SBPay > Reports > Significant Balances for personnel directly involved in compliance or audit tasks. This tool facilitates efficient cross-checking of data and transactions for accuracy and regulatory adherence.

5. Security and Confidentiality Measures:

- Restrict access to report generation tools to authorized personnel.
- Implement encryption for sensitive reports during storage and transmission.
- Use secure file-sharing protocols for external report submissions and only appropriate access rights is given to the recipient.

11. DEFAULT SYSTEM SECURITY FEATURES

11.1 Timed Access (Session Timeout)

- The system automatically logs out after 3 minutes of inactivity to prevent unauthorized access from unattended devices. This feature enhances security by reducing the risk of unauthorized usage.

11.2 One-Time Pin (OTP) Authentication

- An OTP is required to validate all critical transactions, ensuring an additional layer of security. This dynamic code is sent to the registered mobile number or email, mitigating the risk of unauthorized transactions.

11.3 Mobile Device Registration

- Users can only register up to two devices to access their SBPay account. This restriction prevents unauthorized device access and enhances account security by linking activity to verified devices.

11.4 Balance Limit

- SBPay accounts can hold a maximum of PHP 50,000. This limitation minimizes financial risks associated with unauthorized access or fraudulent activities.

11.5 Hold Amount Facility

- A tool for temporarily holding funds in accounts flagged for suspicious activity. This feature is crucial for preventing unauthorized withdrawals while issues are being investigated.

11.6 Account Locking

- Provides administrators the ability to lock accounts suspected of fraudulent activities or security breaches. Locked accounts remain inaccessible until investigations are complete and resolutions are applied.

11.7 Significant Balance Monitoring

- Transactions involving PHP 50,000 or more, whether as a single transaction or cumulatively, are flagged for monitoring. This ensures timely review of high-value activities for compliance and fraud detection.

11.8   Transaction Reversal

- Enables authorized personnel to reverse transactions when errors or disputes arise, providing timely and informed support to clients while ensuring traceability of actions.

11.9   Two-Factor Authentication (2FA)

- 2FA is seamlessly integrated into SBPay, requiring users to verify their identity through a combination of factors, such as passwords and OTPs, for secure logins and transactions. This ensures enhanced protection against unauthorized access and aligns with SBPay's commitment to robust account security.

11.10   User Alerts

- SBPay ensures users are immediately notified via email or SMS for every transactional activity. This feature enhances security by keeping users informed and enabling prompt action in case of unauthorized activity.

ENCRYPTION IN SBPAY USING AWS SERVICES:

To ensure data security, SBPay leverages AWS encryption mechanisms to protect sensitive information both in transit and at rest:

11.11   Root Account / IAM User

- IAM users in SBPay are provisioned according to predefined security levels**,** ensuring access aligns with specific roles and responsibilities.
- Access permissions follow the principle of least privilege, granting only the necessary rights based on operational functions.
- System administrators are granted full access to configurations, audit logs, and system settings for management and oversight.
- This role-based access control structure enhances security**,** supports operational integrity, and ensures compliance

11.12   Encryption in Transit

- **AWS Certificate Manager (ACM):** Utilized to manage SSL/TLS certificates, enabling secure HTTPS communication between client devices and SBPay servers.
- **Transport Layer Security (TLS):** Ensures data integrity and confidentiality during transmission by encrypting data exchanged between users, applications, and servers.

11.13   Encryption at Rest

- **AWS Key Management Service (KMS):** Manages encryption keys to encrypt data stored in databases, object storage (e.g., Amazon S3), and backups.
- **Amazon RDS and S3 Encryption:** Ensures that sensitive customer data in databases and files is encrypted using AWS-managed keys or customer-managed keys.

11.14   End-to-End Encryption Strategy

- Combines encryption in transit with encryption at rest, ensuring comprehensive protection throughout the data lifecycle.
- Sensitive operations like transactions and user authentication are secured by encrypting payloads using secure algorithms (e.g., AES-256).

11.15   Compliance and Monitoring

- **AWS CloudTrail:** Tracks encryption key usage and access for compliance auditing.
- **AWS Config:** Monitors resource configurations to ensure encryption policies are enforced consistently.