Standard Operating Procedure (SOP): Payment Processing and Method Verification Procedures

This SOP details the **payment processing and method verification procedures** to ensure accurate, secure, and efficient handling of financial transactions. It covers steps for verifying payment methods, processing payments through various channels, preventing fraud, maintaining transaction records, and resolving payment discrepancies. The objective is to safeguard financial operations, enhance customer trust, and comply with regulatory standards.

1. Purpose

This SOP establishes standardized procedures for processing payments and verifying payment methods to ensure security, accuracy, and compliance with relevant regulations.

2. Scope

This SOP applies to all staff involved in receiving, verifying, and processing payments through any channel (online, POS, phone, mail, etc.).

3. Definitions

Term	Definition
Payment Processing	The act of accepting and completing a financial transaction.
Payment Method Verification	The steps taken to ensure a payment instrument is valid and authorized for use.
Discrepancy	Any mismatch or error detected in payment amount, method, or processing.

4. Responsibilities

- **Finance Department:** Oversees payment processing and ensures adherence to SOP.
- **Cashiers/Payment Handlers:** Conduct payment acceptance, verification, and record-keeping.
- **Supervisors/Managers:** Monitor compliance and investigate discrepancies.

5. Procedure

1. **Payment Method Verification**
   - Confirm customer identity where applicable (photo ID, account details).
   - Inspect payment instrument (card, check, digital wallet, etc.) for validity and expiration.
   - For cards: Match cardholder name, check security features (EMV chip, signature, etc.).
   - For checks: Verify check authenticity, account status, and sufficient funds.
   - Electronic payments: Use secure gateways; require multi-factor authentication as available.

2. **Payment Processing**
   - Enter transaction details accurately into the designated system.
   - Process payment via approved channels (POS terminal, online portal, bank transfer).
   - Obtain system or bank authorization for all transactions.
   - Provide customer with a receipt or transaction confirmation.

3. **Fraud Prevention**
   - Monitor for suspicious activity (unusual amounts, repetitive attempts, etc.).
   - Escalate suspected fraud to management and follow anti-fraud protocols.
   - Do not process payment if verification fails or fraud is suspected.

4. **Transaction Record-Keeping**
   - Maintain accurate transaction records in the main system and backup as required.
   - Store sensitive payment data securely and in compliance with data protection laws (e.g., PCI DSS).

5. **Discrepancy Resolution**
   - Investigate any identified discrepancies in payment amounts, duplicates, or method.
   - Document investigation steps and outcomes.
   - Report unresolved discrepancies to the finance manager for review.

6. Compliance and Security

- Adhere to applicable laws and regulations governing payment processing (e.g., PCI DSS, AML, KYC).
- Ensure all staff are regularly trained on payment security and fraud prevention.
- Periodically review and update procedures to address new risks or regulatory changes.

7. Revision & Review

- This SOP should be reviewed annually or upon significant change to payment technologies or regulations.
- Document all SOP revisions with date and description of changes.

8. References

- Payment Card Industry Data Security Standard (PCI DSS)
- Anti-Money Laundering (AML) Regulations
- Internal Company Policies