SOP Template: Modes of Payment Acceptance and Processing

This SOP details the **modes of payment acceptance and processing**, covering various payment methods such as cash, credit and debit cards, mobile payments, and online transactions. It outlines procedures for verifying payment authenticity, handling refunds and chargebacks, ensuring secure data handling, complying with financial regulations, and reconciling daily transactions. The aim is to provide a seamless, secure, and efficient payment experience while minimizing errors and fraud risks.

1. Scope

This SOP applies to all employees involved in the acceptance and processing of customer payments across all sales channels and platforms.

2. Accepted Payment Methods

Payment Method	Channel(s)	Description
Cash	In-store/On-premises	Physical currency notes and coins
Credit Card	In-store, Online, Mobile	Visa, MasterCard, American Express, etc.
Debit Card	In-store, Online, Mobile	Maestro, Visa Debit, etc.
Mobile Payments	In-store, Online, Mobile	Apple Pay, Google Pay, Samsung Pay
Online Wallets	Online	PayPal, Stripe, etc.
Bank Transfers	Online	Direct account-to-account transfers

3. Payment Acceptance Procedures

- **Cash:** Count cash in front of the customer, provide a receipt, and store securely.
- **Card Payments:** Confirm card ownership (e.g., signature, ID if required), securely process via terminal, return card to customer, and issue receipt.
- **Mobile/Online Payments:** Ensure transaction confirmation is received before releasing products or services.
- **Bank Transfers:** Verify receipt of funds in business account prior to order fulfillment.

4. Payment Verification and Fraud Prevention

- Inspect all physical bills and coins for authenticity using counterfeit detection tools as needed.
- For card payments, match cardholder signatures or IDs where possible; follow PCI DSS compliance for card data handling.
- Use fraud detection software for online payments; flag and investigate high-risk transactions before approval.

5. Handling Refunds and Chargebacks

- Process refunds to the original payment method only after verifying the transaction.
- Document reasons for refund or chargeback and obtain necessary approvals.
- Respond promptly and cooperatively to chargeback notifications following established dispute process.

6. Secure Data Handling

- Never record or store full card numbers and sensitive customer data unless required and permitted.
- Adhere to industry standards (e.g., PCI DSS) for all card processing hardware/software and data storage.

- Limit access to financial data to authorized personnel only.

7. Regulatory Compliance

- Follow all local and international financial regulations (e.g., anti-money laundering, Know Your Customer).
- Retain transaction and refund records per legal retention guidelines.

8. Daily Reconciliation and Reporting

- Reconcile all payments at the end of each business day against transaction records and POS/system reports.
- Investigate and resolve discrepancies immediately; document all findings.
- Generate and archive daily reports for management review.

> **Note:** All employees handling payments must complete relevant training in transaction processing, security protocols, and fraud detection as part of onboarding and annually thereafter.

9. Review and Updates

This SOP shall be reviewed annually or upon significant changes in payment mechanisms, regulatory requirements, or business operations.