# Standard Operating Procedure (SOP): Order Payment Confirmation and Fraud Check

This SOP details the **order payment confirmation and fraud check** process, including verifying payment details, validating transaction authenticity, cross-checking customer information, monitoring for suspicious activity, and ensuring secure payment processing. The goal is to prevent fraudulent transactions, confirm legitimate payments, and maintain the integrity of the order fulfillment system.

## 1. Purpose

To outline the standard process for confirming payment for customer orders and performing fraud checks to detect and prevent fraudulent transactions.

## 2. Scope

This procedure applies to all customer orders where online payment is collected, for both physical and digital products/services.

## 3. Responsibilities

- Payment processing team: Execute payment confirmation and fraud checks.
- Customer service team: Communicate with customers in case of flagged issues.
- Fraud prevention specialist: Analyze and resolve suspicious transactions.

## 4. Procedure

1. **Payment Receipt**
   Receive payment confirmation from the payment gateway/system for each order placed.
2. **Verify Payment Details**
   - Check that the amount received matches the order total.
   - Ensure payment method (credit card, PayPal, etc.) matches customer file.
   - Verify transaction timestamp aligns with order creation.
3. **Validate Transaction Authenticity**
   - Confirm transaction ID/reference number with payment provider.
   - Check confirmation codes or digital signatures as applicable.
4. **Cross-Check Customer Information**
   - Compare billing and shipping addresses for consistency.
   - Match customer name, email, and phone with account records.
   - Review order history for irregularities.
5. **Monitor for Suspicious Activity**
   - Flag orders with unusually large values or multiple payment attempts.
   - Identify mismatched location/IP address and customer profile data.
   - Scan for blacklisted card numbers or users.
6. **Flag and Escalate Suspicious Transactions**
   - Hold fulfillment for flagged orders.
   - Notify fraud specialist for verification and resolution.
   - Contact customer for additional verification if necessary.
7. **Confirm Legitimate Payments**
   - Clear order for fulfillment and processing once payment is confirmed and no fraud detected.
   - Update order status to "Payment Verified."
8. **Document and Report**
   - Log payment confirmation and fraud check in order management system.
   - Maintain records for audit and review.

## 5. References

- Payment Gateway Fraud Prevention Guidelines
- Internal Fraud Response Protocol
- Data Security and PCI Compliance Policy

## 6. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 2024-06-20 | 1.0 | Initial SOP created | Compliance Team |