Chargeback Policy

1. Purpose

The Chargeback Policy outlines the procedures and guidelines for handling chargeback requests initiated by customers of GCCH Management FZE ("the Company"). Chargebacks occur when customers dispute a transaction and request their issuing bank to reverse the payment.

2. Chargeback Process

2.1 When a customer initiates a chargeback request with their issuing bank, the Company will receive a notification from the payment network.

2.2 The Company's dedicated chargeback team will promptly review the case, gather relevant transaction information, and assess the validity of the dispute.

2.3 If the Company determines that the chargeback is valid and the customer is entitled to a refund, the necessary funds will be debited from the merchant's account, along with any associated chargeback fees.

2.4 If the Company believes the chargeback is invalid, the chargeback team will compile evidence to support its stance and respond to the payment network within the required timeframe.

2.5 The Company will maintain clear documentation of all chargeback cases, including evidence, communication with customers, and responses to payment networks.

3. Prevention Measures

3.1 The Company will implement robust transaction monitoring and fraud detection systems to identify potential fraudulent activities and prevent chargebacks.

3.2 Transparent communication with customers, clear billing descriptors, and easy-to-access customer support will reduce confusion and minimize disputes.

3.3 Regular merchant education on best practices for preventing chargebacks will be conducted to maintain a low chargeback ratio.

Risk Management

1. Purpose

The Risk Management Policy outlines the procedures and strategies for identifying, assessing, and mitigating risks associated with payment processing activities of GCCH Management FZE.

2. Risk Identification and Assessment

2.1 The Company will continuously monitor and assess risks associated with transactions, merchants, and other aspects of payment processing.

2.2 Risk assessment will involve evaluating factors such as transaction volume, geographic location, industry, and historical data.

2.3 The Company will use data analytics and AI-driven tools to identify patterns indicative of potential fraud or high-risk activities.

3. Mitigation Strategies

3.1 A tiered risk assessment framework will be established to categorize merchants based on their risk levels.

3.2 High-risk merchants will be subject to enhanced due diligence, periodic reviews, and additional transaction monitoring.

3.3 The Company will maintain relationships with reputable third-party risk assessment providers to ensure accurate risk evaluations.

4. Incident Response

4.1 The Company will develop an incident response plan to address potential breaches, fraud attempts, or other security incidents promptly.

4.2 The incident response plan will involve notifying relevant parties, initiating investigations, and implementing corrective actions to prevent future occurrences.

Fraud Prevention Policy >

Fraud Prevention Policy

1. Purpose

The Fraud Prevention Policy outlines the strategies and measures to detect, prevent, and mitigate fraudulent activities within the payment processing operations of GCCH Management FZE.

2. Fraud Detection

2.1 Advanced fraud detection algorithms and machine learning models will be employed to analyze transaction data in real-time for unusual patterns.

2.2 High-risk transactions will be flagged for manual review by the fraud prevention team.

3. Fraud Prevention Measures

3.1 Multi-factor authentication and secure payment gateways will be implemented to verify the identity of customers and merchants.

3.2 Regularly updated lists of known fraudulent accounts and activities will be used to identify and block suspicious entities.

4. Collaboration and Reporting

4.1 The Company will collaborate with law enforcement agencies, industry peers, and payment networks to share information about emerging fraud trends.

4.2 Comprehensive fraud reports will be generated periodically to assess the effectiveness of fraud prevention measures and make necessary adjustments.