FIS Merchant Solutions

Best Practices for Fraud Prevention

Reference Guide for Merchants

This document is not meant to be a detailed description or a complete listing of all requirements or of your obligations. We urge you to read your Merchant Agreement, the rules and regulations of the Card Associations and applicable law in order to understand fully all of your obligations as a merchant accepting card transactions and, if appropriate, consult with your own legal advisor. We also note that these requirements may change over time, and that you will be responsible for complying with any such changes as they come into effect.

Table of Contents

FIS Merchant Risk Team

FIS™ Merchant Solutions has a dedicated Merchant Risk Team focused exclusively on fraud detection, avoidance, merchant protection and compliance.

Contact Information and Availability

The Merchant Risk Team is available to merchants and FIS staff for risk concerns during the following standard hours of operation:

Monday through Friday
8:00 a.m. – 5:00 p.m. ET.
P: **866.307.4244**
E: BCS.MerchantRisk@fisglobal.com

Tips for the Point-of-Sale

CVV2 (security code on back of card) and AVS (address verification)

Should be completed on all orders. Both should be a positive match.

Excessive Declines

If a transaction is declined, do not attempt to authorize the card more than one time. Instead, request the customer contact their issuing Financial Institution to find out why the card is declining or request another form of payment. Excessive attempts on a card can potentially lead to the card being blocked for suspicion of fraud and/or may indicate that the transaction is fraudulent

Velocity Filters

When utilizing third-party software for payments it is recommended that you contact your software provider and implement Velocity filters, which limit the number of transaction attempts on a card and will help to prevent high-volume attacks common with fraudulent transactions. We recommend this filter be set to allow no more than 2 or 3 attempts in 24 hours. Excessive declines may indicate that a merchant is being tested with fraudulently obtained card numbers. Please also review the E-commerce section further in this guide and recommend fraud filters for all the scenarios.

Swipe or insert versus keyed

Always swipe a non-chip card, or insert a card if chip enabled whenever possible. This proves the actual card was in your possession at the time of the sale.

No Force Posting Transactions

Do not force post a transaction through your terminal. **If a card is declined when you attempt to obtain an authorization, do not make up an authorization code or settle a sale for more than the original authorization was approved.** You could potentially receive a chargeback with a reason code of invalid authorization. Never obtain an authorization code from the customer or from a telephone number or conversation provided by the customer.

Split Transactions

Never split the total sale amount into several transactions. This is often requested to avoid fraud detection tools.

Refunds

Never send funds back to a customer via check or wire transfer. You should always refund a sale the way it was originally processed. You should never issue a credit to any other card then the original card used for the sale.

Settle your terminals daily

This will reduce the possibility of late presentment transactions.

Red Flags for Orders

The following are some of the most common scenarios associated with fraudulent purchases. **Read through each of these tips carefully and consider them when accepting orders.**

Requests for Overnight Delivery

If a customer requests FedEx/UPS overnight delivery and the transaction turns out to be fraudulent, it is likely you will be unable to stop or recall the shipment. You would most likely receive a chargeback and your business will be at a loss for the funds and the merchandise.

Alternate Addresses

Customer requests the product to be shipped to an alternate address/not the billing address (AVS verification).

Change of Plans

Customer originally stating that they will pick up the order and then changes it to a private or national delivery service.

Multiple Orders with Multiple Destinations

Customer requests to have multiple orders shipped to multiple locations.

Suspicious Wording

Email is poorly written (spelling and grammatical errors).

Foreign Orders

Orders from foreign countries if you typically only receive domestic orders.

Unnecessary Orders

Orders that easily could be obtained at a larger retailer within the cardholders billing area if you are in a rural area.

Excessive Orders

Excessive orders for identical products (5 to 10 orders for the same item).

Multiple Declines

Multiple declines received when attempting to process the transaction.

Multiple Cards Used

Customer provides multiple card numbers to pay for orders.

Special Shipping Requests

Customer requesting to use their own shipping company.

Freight Requests

Customer requests merchandise shipped to a freight loader and requests reimbursement of freight charges.

First Time Customers Insisting to Pay by Credit Card

Be cautious if you receive an order from a customer using a telephone relay service.

E Commerce Orders

Take caution with orders that are placed with you online. In particular, watch for the following:

- Multiple cards used from the same IP address
- Same name or email address used for multiple orders using different card numbers
- Multiple orders being shipped to different addresses

Tips for Chargeback Avoidance

Most chargeback situations arise at the time the transaction is completed and most can be prevented with a little training. Here are some tips to avoid potential chargebacks:

- Do not complete a transaction if the authorization request was declined. If a decline response is received during a transaction, ask the card holder for another form of payment. If the transaction was processed with a decline response, you are responsible for the chargeback.
- If you received a “Call” message in response to an authorization request, call your Authorization Center. This number is listed on your terminal sticker.
- Ensure that transactions are entered into point-of-sale terminals only once, and deposited only once.
- If your establishment has policies regarding merchandise returns or service cancellations, disclose these policies to the cardholder at the time of the transaction.
- Settle transactions daily.
- Keep your customers updated on the status of their order.
- If a retrieval request is received, always complete the rebuttal or it could result in a Chargeback.