"BEST PRACTICES TO ACCEPT PAYMENTS ONLINE"

Below mentioned are the best practices employed in Asia Pacific on online merchant transactions in the Card-Not-Present scenario. UBL recommends merchants to follow these best practices in order to minimize exposure to the fraudulent transactions.

BASIC BEST PRACTICES

1. Strict Registration Policy:

At the online portal, it is important to ensure that merchant gather sufficient information of customers. Key best practices at the point of user registrations include

a) Mandating customer registration.

This should include mandatory customer information such as;

- Customer Name
- Telephone number & Mobile Number
- E-mail address
- Date of birth
- Residential address
- Billing Address
- Shipping address
- CNIC number / Passport number

2. Active Monitoring

Apart from implementing strict user registration policies, merchants must also actively monitor all transactions. Merchant should maintain the Positive, Negative and Blocked list of its customers. Best practice tactics in this area include:

a) Stricter criteria for making payment through cards:

Merchant should limit transaction count and number of unknown users (i.e. those that are not on the positive list or are not registered with the merchant or have just registered and attempting their first transaction). This is usually done by setting a low limit of transaction for new user IDs and implementing a daily and monthly limit on both the user ID level and IP address level. Transaction from the blocked list should simply be declined. We recommend for following limits

- Positive List:
  Min. transaction amount PKR XXX/- (as per merchant's business requirement)
  Max. transaction amount PKR XXX/- (as per merchant's business requirement)
  Maximum number of transaction(s) per month 3(three)

- Negative List:
  Min. transaction amount PKR XXX/- (as per merchant's business requirement)
  Max. transaction amount PKR XXX/- (as per merchant's business requirement)
  Maximum number of transaction(s) per month 1(one)

Minimum and maximum transaction amount capping is dependent on merchant's transaction volume. Transaction size should vary between positive list and negative list.

Payment gateway portal doesn't provide merchants access to customer debit / credit card number. However merchants are provided with the **Card Token** which is the unique card number mapped with each credit / debit card. Merchant can use the card token to identify the frequency of the transactions occurred through a particular card on its website. Merchant can verify the frequency & consolidated amount of the transaction attempted on merchant website in a defined tenure and then take decision to accept or decline the transaction. To make this functionality available systematically while processing transactions through payment gateway, please review below link:
https://demo-ipg.comtrust.ae/merchant/downloads/EPGFraudDetection.pdf

b) Transaction verification with "positive-list" and "negative-list":
Merchant should maintain a "positive-list" of genuine past users that frequently transact on card. Transactions from these customers may not be routed through the risk filters to avoid unnecessary service issues with these regular customers. (Use prior cardholder purchases as a favorable factor to apply less restrictive screening and review when cardholder information has not changed). Similarly, a "negative-list" of customers and transaction attributes of previously suspicious transaction should be maintained. Key attributes that can be maintained for the "negative-list" include IP addresses, customer names, card accounts (truncated), card token, cardholder names, mobile numbers and email addresses etc.

3. Preventive Actions

Apart from ensuring strict registration of your customers and active monitoring, it is important to take strong preventive actions on detected suspicious transactions. Best practices in this area include:

a) Account closure:
Suspicious accounts detected either via positive match with the negative list database must immediately be suspended. A look-back for all other accounts with similar attributes such as the same IP address, credit card account numbers should be immediately blocked.

HOW TO REDUCE SUSPICIOUS TRANSACTIONS

I. Screening for High-Risk Transactions:

a) Implement fraud-screening tools to identify high-risk transactions:
Suspend processing for transactions with high-risk attributes. This can include transactions that

- Match data stored in your internal negative files
- Exceed velocity limits and controls
- Match high-risk profiles
- Be on the lookout for customers who use anonymous e-mail addresses

Develop effective and timely manual review procedures to investigate high-risk transactions. The goal here is to reduce fraud as a percentage of sales and minimize the impact of this effort on legitimate sales.

b) Treat international IP addresses and high value transactions as higher risk:

Treat international IP addresses as higher risk. Merchants have found that international IP addresses have a substantially higher fraud rate than domestic addresses. By classifying international IP addresses as higher risk, you can require these transactions to meet higher-risk hurdles. For example, to call back on customer's provided number and investigate about provided information and cross check with the information provided on the website. Merchant should also require shipping address to match with billing address for higher risk transactions.

c) Screen for high-risk shipping addresses:

Merchant can reduce fraud by comparing the shipping address given by the customer to high-risk shipping addresses in third party databases and in your own negative files.

- Pay special attention to high-risk locations such as mail drops, prisons, hospitals, and addresses with known fraudulent activity.
- Treat transactions from international cards and shipment to international address as higher risk
- Thoroughly scrutinize or restrict shipping merchandise to foreign addresses
- Consider curtailing shipments of merchandise to higher risk countries.

II. Analyzing questionable transactions

a) Develop/maintain customer database:

Develop/maintain customer database or account history files to track buying patterns. Compare/evaluate individual sales for these signs of possible fraud

- **Larger-than-normal orders:** Because stolen cards or account numbers have a limited life span, criminals need to maximize the size of their purchase.
- **Orders consisting of several of the same item:** Having multiples of the same product increases fraud risk.
- **Orders made up of "big-ticket" items:** They offer maximum resale value and profit potential
- **Orders shipped "rushed" or "overnight":** Criminals want their fraudulently obtained items as soon as possible for a fast resale.
- **Order delivered to new shipping address:** 1st time shopper
- **Multiple orders placed using different names, addresses, and card numbers, but coming from the same Internet Protocol (IP) address.**
- **Orders shipped to a single address but paid for using multiple cards:** These could be generated account numbers or a batch of stolen cards
- **Multiple transactions on one card over a very short period of time:** This could be an attempt to "run" a card until the issuer closes the account

- **Multiple transactions on one card or similar cards with a single billing address, but multiple shipping addresses:** This could represent organized fraud activity
- **Multiple cards used from a single IP (Internet Protocol) address:** This could mean a fraud scheme

III. Establish procedures for responding to suspicious transactions using cardholder verification calls

Contacting customers directly not only reduces fraud risk, but also builds customer confidence and loyalty. Your verification procedures should address both the need to identify fraud and the need to leave legitimate customers with a positive impression of your company.

a) Use directory assistance or Internet search tools:
   Not the telephone number given for a suspect transaction, to find a cardholder's telephone number

b) Confirm the transaction:
   Resolve any discrepancies, and let the cardholder know that you are performing this confirmation as a protection against fraud

IV. Develop Fraud Score

a) Develop a fraud score internally to better target the highest risk transactions which require additional verifications
   - Perform internal fraud screening before submitting transactions for settlement
   - Submit only those transactions that have passed your internal screening

V. Suspect Transaction Review

a) Ensure that all transactions with higher risk characteristics are routed for fraud review such as:
   - Hits against the negative file
   - International IP addresses
   - Foreign billing or shipping addresses

OPTIONS AVAILABLE WHEN YOU SUSPECT FRAUD

- Hold shipment until further verification as defined in document
- Phone cardholder back for verification, in case of suspicious behavior or mismatch of information provided by cardholder on phone to the website, cancel the order and ask to pay through other mode of payment
- Use carrier that requires identification at delivery
- Deliver order to an address not a location
- Know your organization escalation procedures and escalate the transaction suspicious behavior accordingly