Best Practices for Credit Card Acceptance to Minimize Fraud

By implementing best practices in credit card processing, you decrease the likelihood of fraudulent transactions and chargebacks.

In general, transactions fall into two categories:

Card Present - The consumer’s card is presented in a face-to-face environment (retail)
Card-Not-Present – The consumer’s card is not present at the point of sale (website, phone order, etc.)
Card Present Best Practices (Retail)

• **Swipe the card through the point of sale system.**
  ▫ A card that has been “swiped” generally has lower interchange fees than those that are manually keyed. In addition, the customer’s information is automatically captured with that transaction.
  ▫ Avoid key entry whenever possible. If you must enter numbers manually, be sure to get an imprint of the card.

• **Authorize the transaction.**
  ▫ Review the authorization response and take the appropriate action:
    ▪ Approved – Ask the customer to sign the sales receipt.
    ▪ Declined – Return the card to customer and ask for another form of payment.
    ▪ Call or Call Center – Call Vantiv at 1-800-991-9911 for a voice authorization.
    ▪ Pick Up – Keep the card if you can do so peacefully.
  ▫ If at any point you suspect fraud, contact Vantiv for a Code 10 call and follow the operator’s instructions.
Card Present Best Practices (Retail) (Continued)

- Validate the physical card. Ensure the card has not been altered.

- Request a signature and be sure that the signature on the transaction receipt matches the signature on the card.
  - A signature is not always required on certain small ticket transactions. Check with Vantiv for more details.

- Settle the transactions daily.
  - Authorizations that are not settled within a day will receive a higher interchange rate.
Card-Not-Present Best Practices
(phone order, e-commerce, etc.)

- Authorize the transaction.
  - All transactions must be authorized.
  - Avoid key entry whenever possible. If you must enter numbers manually, be sure to get an imprint of the card.

- Utilize fraud prevention tools such as:
  - Address Verification Service (AVS) to check the cardholder’s address given at the time of the sale against the address on file with the cardholder’s bank.
  - CVV2/CVC2 to verify the security code located on the signature panel of the card. (On American Express cards the number is printed on the front of the card.)
  - If you receive an authorization but are suspicious of fraud, ask more questions.

- Ensure timely processing between the time the order is placed and the time you deliver the goods.
  - Your transaction date should be the same as your shipment date and not be greater than 7 days from the authorization date.
  - Do not charge your customer before you have shipped your goods.

- Identify transactions with the proper card-not-present and e-commerce indicators.

- Settle all transactions daily.
Top 10 Opportunities to Manage Interchange Expense

1. Follow Card Present and Card-Not-Present card acceptance best practices.

2. Avoid key entering transactions at the point of sale.
   - Consider zip code checks at the POS if key entry is necessary.

3. Settle transactions on a daily basis.

4. Authorize all transactions.

5. Utilize AVS and CVV2 on all Card-Not-Present Transactions.

6. Issue all credits back through the same channel in which they were initially processed (do not issue a check refund for a credit card transaction).

7. Consider transmitting Sales Tax, Customer Code, and Line Item Detail (also known as Level II and Level III data on commercial transactions).

8. Always use the most up-to-date equipment or POS software version.

9. Evaluate PIN debit acceptance.

10. Review your reports and transaction data regularly and report any issues to Vantiv.
Top 10 Tips for Chargeback Prevention

1. Do not complete a transaction if the authorization request was declined.

2. If you receive a referral message in response to an authorization, call 1.800.991.9911 for a voice authorization.

3. Get a cardholder signature on all card present transactions.

4. Make sure transactions are deposited only once.

5. Explain your policies regarding returns, refunds, or service cancellation to the cardholder at the time of sale.

6. Process credits in a timely manner.

7. Respond to the requests to cancel recurring payment transactions immediately, or as specified by the customer.

8. Make sure that the merchant name that appears on the customer’s statement is recognizable to the customer. If not, advise the customer what he/she should expect on their credit card statement.
Fraud Prevention

Fraud can occur at any time, whether you’re using card present or card-not-present processes. There are some warning signs that can help identify potential fraudulent activities.

Be aware of customers who:
1. Purchase a large amount of merchandise:
   - Without regard to size, style, color, or price
   - At the time the store is closing
   - With many of the same items purchased multiple times

2. Request overnight or rush shipping for delivery items.

3. Are first time shoppers.

4. Make card-not-present transactions using very similar card numbers.
Tools to Prevent Fraud

Card Verification Code (also referred to as CID, CVV2, CVC2, CSC)
• The card verification code is a 3 or 4 digit value printed on the card or signature strip, but not encoded on the magnetic stripe. It is used on card-not-present transactions to verify that the person actually has the card and not just a stolen credit card number.

• Merchants are not allowed to store this information on their database, it is only used to authorize the transaction and then the response code (i.e. “match” or “does not match”) is stored in the database. It is important to not only send the card verification code with the authorization request, but also to systematically decline all transactions where the code does not match.

AVS (Address Verification)
• AVS requires the customer to input their street number and zip code, and is typically used on Ecommerce transactions, but can be helpful on any transaction where the card is not swiped. The street number and zip code are matched to the billing address associated with the card. Again, it is important to not only capture the address information, but to systematically decline all transactions that are not a match.