Counterfeit Fraud Mitigation Best Practices

Point-of-Sale Merchants Who Are Not EMV® Chip Enabled

Point-of sale (POS) merchants who have not implemented EMV chip acceptance technology face an increasing threat of counterfeit fraud and resulting associated dispute liability on their transactions. Here are four best practices that you can implement to help reduce counterfeit fraud for POS transactions.

BEST PRACTICE

Read and Compare Verification

Implement Read and Compare verification when:

- Processing transactions over a specific dollar amount
- Purchases involve items known to be associated with high fraud
- The transaction is suspicious

Read and Compare verification can be performed either manually or through your POS device.

Manual Read and Compare

After swiping the card:

This is most effective when sales associates confirm the last four card digits on their own rather than asking the customer to read the numbers aloud.

1 Read the last four (4) digits of the account number on the **physical card.**

2 Compare them to the last four digits appearing on the **receipt**.

Automated Read and Compare Through Your POS Device

(If the necessary software modifications have been made)

- When prompted, input the last 4 digits of the account number
- The device will perform the **Read and Compare** verification

If the numbers	Then
Match	Complete the transaction
Do not match	• Cancel the transaction, **and** • Ask for another form of payment

BEST PRACTICE

Be on the Lookout for Highly Suspicious Transactions

In addition to following all standard card acceptance procedures, you should be on the lookout for suspicious transactions involving:

- High value purchases such as electronics, jewelry or large amounts of merchandise with seemingly no concern for size, style, color, or price
- Use of gift cards to purchase high-end items

Of course, peculiar behavior such as this should not be taken as automatic proof of criminal activity. Use common sense and appropriate caution when evaluating any customer behavior or other irregular situation that may occur during a transaction. You know what kind of behavior is normal for your particular place of business.

BEST PRACTICE

Check the Cardholder's ID if Necessary

If a transaction is suspicious, ask the cardholder for an official ID to help reduce the possibility of fraud. However, it is important to remember that a Visa merchant must not require a cardholder to provide supplemental information such as government ID, driver's license, etc. as a condition of honoring the card.

If you are suspicious about the transaction or feel you need additional information to ensure the identity of the cardholder, adhere to your merchant store procedures and respond accordingly.

BEST PRACTICE

Perform Velocity Checks

Use velocity checks to track the number of transactions associated with a credit or debit card within a specific timeframe (e.g., within a 24 hour period). This functionality allows you to identify how many times a customer has used a card at your store location(s), spot excessive transaction activity, and potentially lessen the opportunity for fraud.

BEST PRACTICE

Establish a Strategy for Risky Self-Service Transactions

Force higher risk transactions (e.g. gift card sales) away from self-service kiosks and into manned lanes, or have your managers review these transactions.

For More Information

To learn more about fraud prevention at the merchant point of sale, visit Visa.com, or contact your merchant bank.