ElectronicPayments®

CHARGEBACK BEST PRACTICES – CARD PRESENT TRANSACTIONS
For Point of Sale and Brick & Mortar Merchants

Electronic Payments has recently noticed an increase in chargebacks resulting from improper transaction handling at the point of sale. This guide outlines essential best practices to help merchants reduce fraud risk, prevent chargebacks, and minimize financial liability.

CARD ACCEPTANCE GUIDELINES

Businesses accepting Visa, Mastercard, American Express, and Discover are expected to follow all applicable card network rules and industry standards, including, but not limited to, those outlined below.

1. EMV Chip Card Transactions
    - Always insert the chip card into the terminal when a chip is present.
    - Never bypass the chip by swiping the card unless specifically directed by the terminal.
    - If the chip cannot be read after multiple attempts, request an alternative form of payment.
    - Do not manually key-enter a card number as a substitute for a failed chip read.

IMPORTANT! Failure to properly process EMV chip transactions may result in liability shifting to the merchant in the event of a chargeback.

2. Contactless & Mobile Wallet Transactions
    - Accept tap-to-pay (contactless) and mobile wallet transactions whenever possible. These payment methods provide enhanced security and reduce fraud exposure.
    - Ensure equipment is properly configured and does not support offline contactless approvals.
    - If the contactless payment is declined, attempt the EMV chip transaction or request another form of payment.

IMPORTANT! Never manually key-enter a card, even for convenience. Manually entered transactions carry high fraud risk, are difficult to dispute in chargebacks, and leave the merchant financially liable, even when AVS and CVV data are present. Always request an alternative form of payment instead of key-entering a transaction.

Strict Prohibitions

Merchants should NEVER:

- Manually key-enter card data including, but not limited to, un-embossed cards
- Write card numbers on paper drafts or receipts
- Take photos of credit cards
- Store cardholder data outside of approved, PCI-compliant systems

IMPORTANT! Handwritten or stored card data does not provide protection in the event of a chargeback and may create additional compliance risks.

FRAUD PREVENTION AT THE POINT OF SALE

Suspicious Transactions

If a transaction appears suspicious:

- You may request a valid form of identification to help verify the cardholder's identity.
- If identification is voluntarily provided by the customer, compare the cardholder name on the card to the identification presented.

Note: Card network rules prohibit requiring identification as a condition of accepting a valid payment card. Transactions should not be declined solely because a customer refuses to provide identification.

Red Flags & Fraud Warning Signs

Exercise caution if any of the following red flags are present:

- The customer appears nervous, rushed, or unusually distracted
- Multiple cards are attempted after repeated declines
- The transaction amount is unusually large or inconsistent with normal purchasing behavior
- The customer requests manual entry of card information, even if the purchase will be picked up in person at a later date
- The purchase behavior does not align with normal activity for the merchant location
- The customer asks to bypass standard payment procedures

If suspicious activity is identified, merchants should proceed with caution and consider declining the transaction.

CHARGEBACK TRENDS & PROTECTING YOUR BUSINESS

Several factors are contributing to the increase in chargebacks, including:

- Manual entry of card numbers
- Failure to process EMV chip-enabled transactions properly
- Improper handling of suspicious transactions

To help reduce fraud exposure and reduce disputes, follow these essential tips:

DO

- Accept EMV chip or contactless payment methods
- Follow proper card acceptance procedures and all terminal prompts
- Train employees on fraud prevention and suspicious transaction handling
- Maintain compliance with card brand and PCI security requirements
- Review card brand chargeback best practices regularly

DO NOT

- Manually key-enter card numbers

- Store or record cardholder data
- Ignore suspicious customer behavior
- Bypass EMV chip or contactless processing procedures
- Assume a transaction is legitimate without proper verification

CARD BRAND RESOURCES

- 🔗 https://www.mastercard.com/us/en/business/support/rules.html
- 🔗 https://corporate.visa.com/en/solutions/acceptance/chargebacks.html
- 🔗 https://www.americanexpress.com/content/dam/amex/us/merchant/pdf/US-Disputes-Reference-Guide-Updated.pdf

Key Takeaways

Consistent adherence to proper card acceptance procedures is critical to reducing fraud exposure, preventing costly chargebacks, and protecting your business from unnecessary financial loss.

You should review these guidelines with their staff and apply them consistently at the point of sale.