# Reducing Data Integrity Errors – Fallback Transactions

## Overview

Fallback transactions are the most common cause of Data Integrity Errors and Fees. A "fallback transaction" is when a chip card is processed as a swiped card, instead. Take steps to help reduce these errors and fees:

- **DO** always insert chip cards
- **DO** always ensure your point-of-sale is operating on the most up-to-date software
- **DON'T** allow a chip card to be inserted improperly (upside down, backwards, etc.)
- **DON'T** allow a chip card to be removed prior to the POS prompting for removal

## Fallback Transaction Details

The Card Brands monitor transaction data in an effort to protect cardholders, merchants, processors – everyone involved in the payment chain. Criminals look for pieces of payment data that can be counterfeited, and for loopholes in the transaction stream that can be capitalized on to commit fraud.

The term "Data Integrity" refers to efforts made by the Card Brands and other stakeholders to analyze payment details and merchant identifiers at every stage of the transaction in order to reduce, even eliminate, any opportunities for a fraudster to counterfeit the card or use a loophole to compromise the consumer or merchant's information. In other words, it's imperative to maintain the **integrity** of the **data**.

There are various issues that can cause a Data Integrity Error and the subsequent Data Integrity Fees; but, did you know that the most common cause is fallback transactions, which are typically preventable?

### What is a Fallback Transaction?

A fallback transaction occurs when a chip card is swiped instead of inserted.

Chip cards must always be inserted so that the card's chip and the terminal's chip reader can interact, allowing for a secure, chip transaction to be processed. The magstripe data on chip cards tells the terminal that the card has a chip and should be inserted. If this requirement is ignored and the transaction is still processed as a swipe instead of inserted and processed as a chip transaction, this violation is communicated in the transaction's data and a Data Integrity Error will generate.

### Why is a Chip Transaction Important?

EMV stands for Europay, Mastercard, Visa. These Card Brands, in collaboration with other key industry players, developed chip technology in an effort to **increase card security** and, in particular, **seek to eliminate counterfeit card fraud**. Chip transactions also significantly reduce merchants' chargeback liability.

#### Chip Cards are More Secure in Card-present Transactions

Chip card technology increases the security of card-present transactions because the chip is nearly impossible to counterfeit, unlike magnetic stripes. During a chip transaction, the computer microchip in the card communicates a one-time use code (cryptogram) with the chip reader in the terminal. Every single chip transaction is uniquely encoded. *But, if a chip card is swiped instead of inserted – the advanced security of the chip isn't used!*

# How to Reduce, even Eliminate, Fallback Transaction Data Integrity Errors

## Always Insert Chip Cards

- It is imperative that all chip cards are properly attempted as a chip transaction. When a chip card is initially swiped through an EMV-enabled terminal instead of inserted, the magnetic data tells the terminal that this is actually a chip card and the terminal will prompt for the card to be inserted.
- If you or your cardholder are having a negative experience with the insert process, please contact Merchant Support for additional guidance on chip card processing. It is likely that a few modifications to your terminal settings will improve the experience.

## Always Insert Chip Cards *Properly*

- Ensure that the card is inserted face-up, chip first.
- Ensure that the card is fully inserted; otherwise, errors can occur and falsely trigger the terminal to generate a Chip Read Error.
- If the initial attempt at inserting the card is not successful - remove the card and attempt the chip process again, ensuring that the card is inserted properly.
- DO NOT allow a chip card to be removed before the terminal confirms the transaction is complete and prompts for the removal. Premature removal can cause unnecessary errors.

## Always Operate on the Most Up-to-Date Payment Software

- Terminals that are operating on out-of-date software can sometimes produce invalid transaction errors, including Chip Read Errors. If your terminal is experiencing widespread issues with chip cards, contact Technical Support right away. It is likely that a simple download to update your software will resolve this issue.
- Take steps to ensure you're supporting successful auto downloads to your terminal so that you will always operate on the latest, most secure application. Ensure your auto download feature is enabled, and that the terminal remains powered on and connected so the auto downloads can take place as scheduled. Look for the confirmation print-out from the terminal once these downloads are completed and contact Technical Support for assistance if the printout indicates that the download was not successful.

# Valid Fallback Transaction

The only scenario where a fallback transaction would be valid is if the card's chip is damaged. In this case, you as the merchant, can either:

- Allow the transaction to process as a swipe.

  or

- Ask the customer for another form of payment.
  - The cardholder will need to notify their issuer that the card's chip is damaged and request a new card.