Mitigating Fraud on Chip Fallback Transactions

To help mitigate counterfeit fraud associated with chip fallback transactions, we recommend the following set of best practices for merchants, including monitoring the terminal's performance to ensure optimal transaction processing, performing the fallback transaction on behalf of the cardholder when necessary and scrutinizing high risk transactions at the point of sale when fallback occurs.

For More Information

To learn more contact your Visa representative.

Although we have seen an overall decline in chip fallback transactions, fraud associated with fallback transactions is on the rise. Fraudsters are devising ways to force fallback transactions, usually associated with counterfeit cards.

The fraudsters' methods target the card or the card insertion process with the terminal which are impacted to bypass a chip read and force a magnetic stripe read on a chip capable card at a chip capable terminal. These methods include:

- **Card containing a blank chip** – No chip read possible
- **Card containing a chip with no matching AID for the terminal to process** – No chip read possible
- **Card contains clear tape or coating over the chip** – No chip read possible
- **Card inserted upside down or backwards into the terminal** – No chip read possible

BEST PRACTICE

Monitor Terminal Performance

Either systemically or through cashiering staff, monitor each terminal's performance. If a terminal or set of terminals are malfunctioning resulting in a larger than expected number of fallback or key-entered transactions, please contact your acquirer or servicer to correct the issue as soon as possible.

BEST PRACTICE

Set Attempted Chip Reads Counter to Allow 2 or 3 Attempts Prior to Falling Back to Magnetic Stripe

To avoid unnecessary fallback transactions, configure the terminal to allow two or three chip read attempts prior to reverting to a magnetic stripe read transaction. This should help address erroneous insertions and partial chip reads to possibly reduce the number fallback transactions originating from your place of business.

BEST PRACTICE

Monitor Fallback Volumes

Similar to the best practice, Monitor Terminal Performance, monitor the volume of fallback that occurs at your place of business. There will always be the rare occasion when a cardholder presents a malfunctioning chip card or perhaps there is an errant insertion by a legitimate cardholder. Either systematically or through cashier staff, track fallback transactions associated with your business. Your acquirer or merchant processor may be able to track and provide you with your business' fallback statistics. In addition to monitoring fallback, track issues with your terminals and chip cards to ensure ongoing terminal performance. If irregularities are discovered, contact your acquirer or servicer to address the terminal issue.

BEST PRACTICE

Have the Cashier Perform the Fallback Transaction and Review the Security Features of the Card

If you have a cardholder facing terminal/key pad and the cashier notices what appears to be multiple unsuccessful chip reads, instruct the cashier to ask the cardholder for the card and perform the transaction for them. Prior to inserting the card into the terminal, the cashier must review the security features of the card. Reviewing the card's security features include:

- Does the chip appear/feel undamaged and uncovered (no tape or clear coating over it)?
- Are the first four digits of the card number printed under the account number on the card?
- Does the hologram function/display correctly?
- Is there a valid Expiration/Good Thru Date embossed on the card appearing below the account number?

If the card passes the security features review, the cashier should insert the card and attempt a final chip read. If the chip read is unsuccessful, the cashier should follow the prompts on the terminal and conduct a fallback magnetic stripe read transaction. If the card does not pass the security features review, for the cashier should request a different form of payment from the cardholder.

BEST PRACTICE

Perform a Read and Compare Verification on Fallback Transactions

Read and Compare verification can be performed either manually or through your business' point of sale (POS) device.

Manual Read and Compare

After swiping the card as part of a fallback transaction:

1. Read the last four (4) digits of the account number on the physical card.
2. Compare them to the last four (4) digits of the account number appearing on the receipt.

As discussed above, the cashier should conduct the magnetic stripe fallback transaction and for the compare, confirm the last four card digits on card match the last four digits appearing on the receipt. Merchants are discouraged from having the cardholder perform the fallback transaction and from asking the customer to read the last four numbers on the card aloud to be used in the comparison.

Automated Read and Compare Through Your Business' POS Device

It may be possible for your POS system to be configured for an automated Read and Compare function. As discussed above, the cashier should conduct the fallback transaction and for the compare, input the last four digits of the account number, when prompted. The device will perform the Read and Compare verification.

BEST PRACTICE

Evaluate Highly Suspicious Transactions At The Point Of Sale That Result In Fallback

In addition to following all standard card acceptance procedures, you should be alert 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
- Transactions that are unusual for your place of business with an unusually high dollar amount and/or a high quantity of items to be purchased that result in a fallback transaction.

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

BEST PRACTICE

Check the Cardholder's ID if Necessary

If a fallback transaction is suspicious, ask the cardholder for an official identification 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 Fallback Velocity Checks

If your POS system provides analytics and management reporting tools, use velocity checks to track the number of fallback transactions associated with a payment 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 specific card at your store location(s) to spot excessive fallback 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) that may result in Other Fallback away from self-service kiosks and into attended lanes, or have the cashier review and if necessary, conduct the fallback transaction.