EMV Implementation Guidance: Fallback Transactions

Version 1.0 – November 2015

Note: This publication is being released for EMV Migration Forum members and their merchant, acquirer, ISV and VAR customers and partners.

The EMV Migration Forum publishes industry guidance on best practices for EMV implementation. The Forum developed this document for merchants, independent software vendors (ISVs), value-added resellers (VARs) and acquirers/processors who may have been experiencing high fallback rates. The guidance outlines potential causes of fallback transactions and actions that can be taken to address the problem.

Fallback Transactions

The payments industry is observing an extremely high rate of fallback transactions coming from newly deployed EMV enabled devices. A fallback transaction normally occurs when a chip card, presented at a chip terminal, cannot be read due to a technical issue with the chip which results in the technology "falling back" to a magnetic stripe transaction. This situation is not expected to occur frequently since the chips on the cards rarely fail. In some situations, a fraudster may create a counterfeit card with an intentionally damaged chip in order to invoke this scenario. For this reason, fallback transactions are deemed risky by the payments industry. Since the issuer holds liability on fallback transactions, they may choose to decline them when they are sent for authorization.

According to the payment networks, a fallback rate of over 2% at one particular merchant or merchant chain is indicative of a problem. The problem may be procedural or related to incorrectly configured POS terminals. Fallback rates over 50% and, in some cases, 100% have been observed in the U.S. since the October liability shift.

A combination of POS entry mode, card service code and terminal entry capability (TEC) is used by the issuer to determine if a transaction is fallback or not. Please refer to payment network specifications for specific values.

Problem: Incorrectly Configured Terminals

A terminal may be incorrectly configured where the terminal is chip hardware capable, but the EMV software and middleware are not yet chip enabled or certified. Specifically, the fallback data indicators in a transaction are being set to values which indicates the terminal is chip enabled.[1] This is very often occurring prior to the required industry test and certification processes being completed successfully. Several variants of this problem are manifesting:

[1] Refer to payment network specifications for additional details on specific values.

1. The terminal entry capability is being set to chip when software or middleware does not support EMV.[2] In addition, the POS entry mode may be erroneously indicating fallback.
2. Specific AIDs are not supported yet on the terminal, or are simply not installed.
3. A phased debit approach is being used where the merchant launches their terminal for EMV credit while still utilizing magnetic stripe for debit.

In addition, other factors may be causing fallback, such as the following;

1. Employees and customers are finding a workaround process to trigger a magnetic stripe transaction while using chip cards at EMV enabled terminals.
2. Host software is incorrectly setting the TEC and/or POS entry mode.

Remedy

To proactively address fallback, acquirers and merchants should consider implementing a monitoring mechanism, identifying merchant locations, terminals or sales associates with high fallback rates. Fallback reporting mechanisms provided by the payment networks and acquiring processors may not be robust enough to identify specific devices in the acceptance environment.

If a terminal exhibits fallback rates of 100%, it is most likely that the terminal is not fully set up to support EMV. Either complete the set-up, or ensure the identifiers within the messages are set to indicate the terminal is magnetic stripe capable only. In some cases, simple hardware upgrades have improperly enabled the chip capability flagging. Note that the identifiers contained within the messages may be improperly set at any processing point between the terminal and the payment network.

Where a phased deployment is underway (by payment network or by debit/credit), on a temporary basis, the terminal/middleware must dynamically alter the identifiers back to magnetic stripe whenever overriding the chip service code. Failure to do so will result in the transaction being incorrectly flagged as fallback. Ensure the identifiers are being set properly for each condition.

When fallback is being experienced:

- Ensure all supported AIDs have been loaded into the device. Some payment networks are associated with more than one AID.
- Provide training to staff on proper EMV processing.
- Review device error logs for intermittent errors.

As defined by EMVCo and the payment networks, fallback should only occur when the terminal cannot read the card's chip due to technical issues with the chip. Any other scenario is not a fallback transaction. If a merchant is using a phased approach to EMV deployment and the merchant chooses to override the chip service code on the card, then (pursuant to EMVCo specifications and/or payment network rules) the terminal must reflect the terminal entry capability as magnetic stripe only. Failure to do so will result in the transaction being incorrectly flagged as fallback.

[2] Note: The terminal entry capability (TEC) value should represent the highest level of capability actively supported by the terminal for each transaction. A terminal's capability must take into account both hardware and software, and should only ever indicate a terminal's true ability to process a payment transaction (i.e., read and transmit full chip data). Acquirers that are beginning to deploy hardware for chip terminals should continue to use the TEC value and/or POS entry mode that indicates magnetic stripe, until the terminal application is enabled to accept chip technology. Once the application is enabled, the TEC should be updated to a value which indicates chip enabled.

Impact and Consequences

There are two widely held beliefs that potentially led to this incorrect implementation:

1. Some merchants/ISOs may have thought that chip hardware is all that is required to protect merchants against liability shift.
2. Merchants, terminal vendors and acquirers may have understood that the TEC/POS Entry Mode reflects the highest level supported by the hardware, when in fact it must reflect the state of the software as well.

Significant and severe consequences for both issuers and merchants, as discussed below, may result, since these incorrectly configured terminals result in extremely high levels of fallback and the incorrect indication that a chip transaction was attempted. This causes a number of issues.

1. High fallback rates may result in compliance action by networks. Consult each payment network to understand fully.
2. Fallback is a high risk transaction often resulting in a decline by the issuer.
3. Fallback is a negative experience for the merchant, cardholder and issuer.

Traditionally during the chip migration period, the vast majority of fallback transactions are attributable to early education/user error issues and technical terminal issues during initial deployment. However, as a result of the large scale problems described in this document, some issuers and merchants are seeing fallback rates as high as 100% at some locations. Globally, fallback rates are under 1% and payment networks are advising strong remedial action for U.S. acquirers with initial rates above a typical market migration rate of 7-10%. As U.S. merchants and acquirers are in various stages of chip migration there may be fluctuations in the number of transactions that appear to be fallback. Previous migrations to chip in other regions have shown that there will be a period of adjustment where the number of fallback transactions will fluctuate.

Problem: Manual Key Entry instead of Following EMV Standard Technical Fallback

There are rare situations where fallback is the only option. However, there is an associated issue that relates to training.

Payment networks have seen merchants going straight to manual key entry when a chip read fails. Given the extremely low probability that both the chip and the magnetic stripe are faulty at the same time, EMV hierarchies of risk management should be followed, with the transaction attempting the next lowest risk transaction. When a chip read fails, the next lowest risk transaction would be a transaction using a magnetic stripe swipe. Fallback to magnetic stripe is more secure than manual key entry and provides more information to the issuer to evaluate the transaction for authorization.

During the migration to chip, merchant staff training regarding following terminal prompts may help to decrease high levels of key-entered transactions. To minimize key-entered transactions, acquirers and merchants should consider implementing a monitoring mechanism similar to the one used for magnetic stripe fallback transactions, identifying merchant locations, terminals or sales associates with excessive rates.

Legal Notice

Merchants, acquirers, processors and others implementing EMV chip technology in the U.S. should consult with their respective payment networks and technical, legal and professional advisors regarding fallback transactions.

While great effort has been made to ensure that the information in this document is accurate and current, this information is provided for informational purposes only, does not constitute legal, technical, implementation or other advice, and should not be relied on for any purpose, whether statutory, regulatory, contractual or otherwise. Always seek the advice of competent advisors prior to making implementation decisions. All warranties of any kind are disclaimed, whether express or implied, including but not limited to warranties relating to or arising in connection with the use of or reliance on the information set forth herein and any implied warranties of merchantability or fitness for a particular purpose. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his, her or its sole cost, expense and risk.

Under no circumstances shall the EMV Migration Forum be liable for any damages whatsoever resulting from the use of or inability to use the information set forth herein (including without limitation, incidental, consequential, indirect or special damages), whether based on warranty, contract, tort, or any other legal theory, and whether or not advised of the possibility of such damages.

About the EMV Migration Forum

The EMV Migration Forum is a cross-industry body focused on supporting the EMV chip implementation steps required for payment networks, issuers, processors, merchants, and consumers to help ensure a successful introduction of more secure chip technology in the United States. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to chip technology in the United States. For more information on the EMV Migration Forum, please visit http://www.emv-connection.com/emv-migration-forum/

Copyright Notice