EMV Troubleshooting Guide for ATM Owners and Operators

Version 1.0

Publication Date: November 2017

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

About the ATM Working Committee

The U.S. Payments Forum ATM Working Committee explores the challenges of EMV migration for the U.S. ATM industry, works to identify possible solutions to challenges, and facilitates the sharing of best practices with the various industry constituents, with the goal result being more positive EMV migration experience for consumers.

EMV is a trademark owned by EMVCo LLC.

Table of Contents

1. Introduction

The implementation of EMV at U.S. ATMs continues at a steady pace. Many ATM owners and operators are now beginning to feel the impact of the U.S. ATM liability shifts. ATM owners and operators are seeing new transaction scenarios and are at risk of incurring chargeback and fallback penalties.

This document provides recommendations to help ATM owners/operators prevent some common transaction problems, and offers suggestions for troubleshooting problems when they do occur.

This document will not cover the dispute process (e.g., chargebacks, re-presentments), since the requirements and policies of industry stakeholders may vary. Consult with the acquirer processor or payment network for specific information about rights and obligations surrounding the dispute process.

The hardware required to support EMV varies based on the ATM manufacturer and model; however, the ATM provider has the responsibility to ensure that all hardware is EMV capable prior to starting EMV implementation.

A recommended best practice is to test the EMV implementation prior to production implementation. This may require test cards[1] with each Application Identifier (AID)[2] supported by the ATM processor. The ATM provider should coordinate testing of EMV functionality at their terminals with their ATM independent sales organization (ISO) or processor, and should explore acquisition of any available test cards with their ATM ISOs or processors, and/or directly with the payment networks.

2. Preventing Common Transaction Problems

Common transaction problems can be prevented by taking steps to ensure data integrity and by monitoring transaction activity.

2.1 Ensuring Data Integrity

It is vital that the data in the transaction request be as accurate as possible, so that an issuer can make the correct authorization decision. An issuer may decline a transaction if transaction data is inconsistent or potentially inaccurate.

2.1.1 Chip Cards at a Non-Chip-Enabled ATM

An ATM that supports only magnetic stripe cards is unable to read the chip on a card. These ATMs can still accept a chip card but the ATM operator will be liable for counterfeit transactions processed on a chip card. ATM operators should ensure that:

- The Track 2 data, including the primary account number (PAN), service code, expiration date, and card security code, is captured from the magnetic stripe and sent "as is" (i.e., unchanged) in the transaction request.

[1] Not all payment networks require physical cards for testing and certification.

[2] See Appendix 1 for information on AID Selection; for information on the U.S. Common Debit AID selection, see the "Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community" white paper.

- The POS Entry Mode accurately reflects the ATM entry capability (magnetic stripe) and that the data was read from the magnetic stripe.
- The transaction code in the request is appropriate for the action being performed (e.g., withdrawal).

2.1.2 Chip Cards at a Chip-Enabled ATM

Prior to deploying or upgrading an ATM in the field, the ATM owner/operator should verify that:

- A valid EMV kernel has been installed prior to loading AIDs. Check with the manufacturer, distributor or other supplier to confirm that the kernel is properly certified and that the certification is current.
- The correct AIDs are configured in the ATM. Obtain and maintain the current AID list from the processor, ISO, and/or manufacturer and make certain that the AIDs are properly loaded in the terminal software.
  - The ATM provider should only implement the AIDs that their acquirer processor supports (i.e., the AIDs for which the processor has completed certification with the relevant payment networks).
- The required EMV tags are passed to the acquirer processor or host system in the transaction request. Do not modify the tag data once the transaction is in flight.
  - Independent ATM deployers (IADs) and ATM providers should work with their ISO, acquirer processor, manufacturer, and/or payment network representatives to ensure that the appropriate fields, and the correct values in each field, are being sent in the transaction message.

Below are examples of transaction types supported by chip-enabled ATMs – full-chip transactions and fallback transactions – and their core data elements. The data elements listed below are not all-inclusive, but have been known to cause problems with ATM deployments in the past. A best practice is to validate these data elements first when problems arise to ensure that they are correct.

Full chip transactions: A full chip transaction is processed when the chip is successfully read and a matching AID is selected:

- The Track 2 data should be obtained from Tag 57 in the chip, and sent “as is” (i.e., unchanged) in the transaction request; the Track 2 data on the magnetic stripe should not be used.
- The Terminal Entry Capability in the transaction request should indicate that the ATM is integrated circuit card (ICC)/chip-enabled.
- The POS Entry Mode should accurately reflect that data was obtained from the chip, not from the magnetic stripe.
- The appropriate EMV data must be included in the transaction request.
  - The exact order or format of these tags/fields may vary, depending on the native mode message format used by the ATM. However, certain fields must always be present if the chip was successfully read and an Authorization Request Cryptogram (ARQC) was generated by the chip. Contact the ISO, acquirer processor, manufacturer, or the relevant payment network specification for additional guidelines.

Fallback transactions: Fallback occurs when a transaction is processed on a chip-enabled ATM, with a chip card, but uses magnetic stripe data. Please refer to individual network rules and specifications for proper handling of these transactions.

- Fallback can be caused for many reasons, including but not limited to: chip card readers not functioning properly; a damaged/malfunctioning chip on a card; and attempted fraud. Additionally, databases in the transaction flow – at a switch, a processor, or an acquirer, for example – may have incorrect Terminal Entry Capability settings that may cause fallback.
  - The Track 2 data should be obtained from the magnetic stripe and sent "as is" (i.e., unchanged) in the transaction request, and the transaction message should reflect that the Track 2 data was obtained from the magnetic stripe, not from the chip.
  - The Terminal Entry Capability data in the transaction request should indicate that the ATM is ICC/chip-enabled.
  - The POS Entry Mode should indicate how the transaction was processed, either chip or magnetic stripe.
  - **Note:** Although an unsupported AID would result in a magnetic stripe transaction, an ATM may incorrectly process this transaction as fallback. Transactions with unsupported AIDs are not valid fallback transactions under payment network EMV specifications.[3]

ATM fallback transactions are typically monitored by the payment networks, and excessive fallback rates may lead to penalties if not corrected. Consult with the processor about the fallback thresholds that have been put in place by the networks and the potential consequences of excessive fallback. Be aware of the policies and how/when excessive fallback notifications occur.

2.2 Monitoring Transaction Activity

In order to gauge the success of the EMV rollout to the ATM fleet, reliable reporting capabilities are important. Prior to implementing EMV, establish a baseline of the current transaction volume so that statistics are available for what is "typical" for a particular ATM (e.g., typical decline rate).

Establish performance thresholds, including:

- Approval/decline rates
- Fallback rates (including approved/declined)
- Percentage of transactions by AID and/or network
- Chip vs. magnetic stripe cards used

Being proactive about reporting will provide critical assistance when problems arise. Don't wait for chargebacks to start rolling in. Look for unusual patterns – for example, low approval rates, excessive fallback – as part of regular reporting.

[3] A non-supported AID does not always equate to fallback. For more extensive information regarding fallback, please see the ATM Working Committee white paper, "Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community" or the U.S. Payments Forum white paper, "EMV Implementation Guidance: Fallback Transactions."

After implementing EMV, thresholds and reporting may need to be modified. Establish a baseline post-EMV implementation so it is clear if performance is improving or getting worse.

Acquirer processors may already be doing this level of monitoring. IADs should check with their ISO or processor to see what monitoring and reporting are performed and available for their ATMs, and what the data and codes indicate. As with the fallback policies mentioned above, it is important to be familiar with the policies and procedures regarding problematic ATM transactions. When will the processor notify the IAD of a potential problem or trend? Will the processor take action before penalties are assessed by the network?

2.3 Additional Recommendations

The following are additional best practices for ATM owners/operators to prevent problems:

- Add periodic cleaning of the chip card reader to the regular maintenance schedule.
- Encourage cardholders, landlords and store personnel to report anything unusual that they or their customers may experience at the ATM.
- Understand what an issuer can charge back, and what is out of scope, for the counterfeit liability shift (e.g., ineligible transactions).
- Review the chargeback process and scope for each payment network supported.
- Be familiar with the entire transaction path once the transaction leaves the ATM. Every switch, processor, acquirer, and payment network is a potential point of failure. Many processors have routing agreements in place that could potentially send one transaction from the ATM down a different path than the next transaction from the same device. Being familiar with these aspects of ATM transaction routing can greatly reduce the time to resolve problems.
- Monitor “Reg E” activity for any unusual trends.

3. Troubleshooting Tips

This section shares common troubleshooting tips used by other providers/deployers in previous EMV deployments on ATMs.

3.1 Determine the Scope of the Problem

When there is an issue, first try to determine the scope of the problem. Some questions to ask include:

- Is the hardware certified to support EMV?
- Is the ATM processing any chip transactions at all?
- Are problems occurring only at a specific ATM, or across multiple ATMs?
    - If at a specific ATM, is the problem happening on all transactions, or is it sporadic?
    - If at multiple ATMs, do they have anything in common (e.g., common kernel, card reader)?
- Are problems occurring only with cards having a specific BIN (i.e., from a particular issuer)?
- Are problems occurring when a specific network is involved, or with all networks?

- Are problems occurring when a specific AID is involved, or with all AIDs?

The cause of the problem, and the appropriate solution, will vary depending on the answers to these questions.

3.2 Watch for Possible Problem Scenarios

This section reviews several problem scenarios that may be seen.

3.2.1 All Transactions Are Being Sent as Fallback

An ATM owner/operator may discover that all transactions initiated by any chip card (not just certain cards or certain BINs) at a specific ATM are being sent as fallback.

- *Potential cause*: Chips are not being read at the ATM because the card reader contacts require servicing.
  - *Solution*: Dispatch hardware vendor to service or replace card reader.
- *Potential cause*: There are data integrity issues. When the transaction reaches the payment network, an incorrect value (e.g., POS Entry Mode, Terminal Entry Capability) is included in the message.
  - *Solution*: Ensure data integrity across all potential points of failure (e.g., card reader, switch, processor) as discussed earlier in this document.
- *Potential cause*: The ATM is not configured properly or the wrong software version is in use.
  - *Solution*: Consult the manufacturer and acquirer processor or ISO

3.2.2 Declined Transactions

A declined transaction does not automatically mean that there is an EMV-related issue. A transaction could be declined for valid reasons (such as insufficient funds or lost/stolen card). These response codes were used pre-EMV and will continue to be valid even after implementing EMV. Troubleshooting and resolving these issues, regardless of the type of card or the ATM capability, should be "business as usual."

3.2.3 Issuer Declines for an EMV-Related Reason

Some common EMV-related reasons for an issuer declining a chip transaction are described below.

- The online ARQC is invalid or chip validation fails. These failures occur for a variety of reasons, including:
  - Key-related issue: Keys or key-related data from the card and in the issuer's hardware security module (HSM) do not match. Alternatively, the card issuer may have a "stand-in" arrangement with a payment network (where the network will approve or decline a transaction on behalf of the issuer if the issuer host is unavailable) and the payment network may have incorrect keys loaded for the issuer.
    - *Resolution*: This is a card issue, not an ATM hardware issue; the ATM provider cannot resolve this problem. The customer should be advised to consult with the card issuer.

- Data integrity issue: All fields required to validate the ARQC were not sent to the issuer (or were dropped before they reached the issuer), so that the issuer did not have the information necessary to validate the ARQC.
    - *Resolution*: Ensure that the card reader is reading the chip correctly and including all chip data in the transaction. If that is verified, work with the acquirer processor or payment network to determine where the chip data was dropped and why. Once a cryptogram is generated, it should not be altered ("stepped on") in any way, by any entity, in the transaction path.

- The issuer did not receive an ARQC, but based on the data in the transaction, they expected one. This failure could be due to any number of reasons, including:
    - Data integrity issue. For example, the combination of the service code in the Track 2 data, the POS Entry Mode, and the Terminal Entry Capability indicator were not logical, or conflicted with other data in the transaction request.
        - *Resolution*: Ensure data integrity as discussed earlier in this document.
    - Missing chip data. A network or other entity in the transaction path dropped the chip data, so it did not reach the issuer. This may occur if an entity in the transaction path is not EMV-enabled.
        - *Resolution*: Work with the acquirer processor or payment network to determine where the chip data was dropped and why.
- The transaction proceeds as technical fallback (a.k.a. "fallback"). Declines by issuers will be dependent on several factors, including: cardholder's transaction history; issuer's risk tolerance; ability to determine if the transaction is a true fallback. Depending on the payment network, these declines may/may not have a specific indicator.
    - *Resolution*: Ensure data integrity as discussed earlier in this document
- The transaction uses an unsupported AID. In this scenario, a chip card is presented at a chip-enabled ATM, but the ATM provider has chosen not to support a specific AID. A magnetic stripe transaction will be created. Based on the data in the transaction request, the issuer is unlikely to be able to differentiate between this scenario and a true fallback scenario; therefore, the issuer may decline the transaction.
    - *Resolution*: If reporting indicates an increase in declined transactions for an unsupported AID, work with the processor, network provider and ATM manufacturer to add the AID at the ATM.
- An invalid routing path is used for the selected AID. U.S. Common Debit AIDs can be routed through any network, while proprietary AIDs may have routing restrictions depending on network routing tables. Transactions that have restricted routing paths may be declined if routed to an unsupported network.
    - *Resolution*: Work with the processor and acquiring network to validate the routing path of the AID being declined.

3.2.4 EMV Chip Transaction Reversal

Once a financial transaction request has been sent, if the transaction cannot be completed, a reversal should be sent to ensure the cardholder's balance is not improperly debited. There are currently no new reversal scenarios as a result of EMV that should be controlled or instigated by the ATM itself.

3.3 Helpful Tips

The following are additional tips to help in determining the root cause of a problem.

- Gather ATM journals/logs and enable extra EMV data logging if available.
- Gather message traces (i.e., message from ATM to acquirer processor or host system). A financial institution will have additional trace data/logs available – such as device handler, authorization, and network interface logs – which may show the message coming into the host and/or the message from the financial institution to the network.
- Develop a good working relationship with the ISO and/or acquirer processor. Know who to contact for assistance with transaction problems.
- Work with the ISO, acquirer processor and/or manufacturer to determine the cause of the problem, since only limited information may be available to the ATM owner/operator. Work with the relevant payment network to analyze and resolve issues whenever possible.
- Train staff so that they are familiar with the format of an EMV/chip transaction and understand the combinations of data that are valid and invalid; staff should also be able to interpret EMV tag data.
- Determine how the transaction was routed. Remember that even transactions from the same ATM may not travel the same path during authorization.
- Work with the relevant payment network to analyze and resolve issues.

3.4 Helpful Resources

The U.S. Payments Forum has published several helpful resources to assist ATM owners and operators with EMV implementation. All resources are available on the U.S. Payments Forum web site at http://www.uspaymentsforum.org

- "Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community" white paper
- "Implementing EMV at the ATM" webinar
- "Implementing EMV in the U.S.: How the U.S. Common Debit AIDs Facilitate Debit Transaction Routing and Ensure Durbin Compliance" video recording
- "Minimum EMV Chip Card and Terminal Requirements – U.S." resource
- "Understanding the U.S. EMV Fraud Liability Shifts" white paper
- GoChipCard.com web site

4. Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Without limiting the foregoing, it is important to note that the information provided in this document is intended only to provide readers with an overview of challenges and issues that its contributors have encountered or believe are likely in connection with implementing EMV at the ATM. Each implementation is different, this document is not intended to be exhaustive, and applicable rules, processing, liability and/or results may impact or be impacted by specific facts or circumstances.

Additionally, each payment network determines its own rules, requirements, policies and procedures, all of which are subject to change.

ATM owners, ATM operators and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with all applicable stakeholders regarding their specific implementation plans and associated rules, requirements, policies and procedures for transaction processing, including but not limited to their respective payment networks, testing and certification entities, and state and local requirements.

5. Appendix 1: Application Selection

Application selection is the process defined in the EMV specifications for a terminal and a chip card to determine if they support any of the same chip applications, and if they do, to agree on which application to use for the current transaction.[4] Application selection is important for several reasons.

- Some applications are suited to ATM, some to the retail point of sale (POS), some to debit, and some to credit. If the card supports multiple applications, different parameters and values may be used for each application. The ATM must use the right information for the transaction being initiated to ensure correct processing.
- Although the global payment network applications support the same basic set of EMV tags (i.e., use the same tag name, tag ID, length, and format), a specific payment network chip specification may also support proprietary EMV tags. For example, a Mastercard application may support a Mastercard-specific EMV tag.
- The format of some EMV tags can vary, depending on the payment network chip specification (e.g., Mastercard M/Chip, Visa VSDC, American Express AEIPS, Discover D-PAS) and the associated application. For the most part, the ATM will simply be transmitting EMV data items to the acquirer for subsequent transmission to the issuer, but particular chip specifications may require the ATM to interpret the data from the chip.
- The ATM owner will be affiliated with some payment networks, but may not be affiliated with others. If the card supports an American Express application, for example, but the ATM does not, then the ATM cannot use the data associated with the American Express application for the transaction. The same is true for all payment networks. This is similar to a magnetic stripe transaction, in that if the acquirer is not authorized to accept American Express cards, the transaction cannot be processed if the magnetic stripe card only supports American Express.

Configuring the ATM to support EMV includes building a list of chip applications (AIDs) that the ATM will support and including that list in the device configuration.

As part of the ATM's EMV configuration, the Application Selection Indicator (ASI) value should be set. This field indicates whether the AID stored in the terminal must be the same length and value as the AID returned by the chip (meaning that only one match can be found for any payment network), or if the terminal can attempt to match by partial AID. It is strongly recommended by the U.S. Payments Forum, and may be required by some payment networks, to always support partial AID selection since this is the only way to support multiple occurrences of applications.

When the chip has been activated, the terminal will build a candidate list, which is a list of all the AIDs that both the terminal and the chip support, and the priority of each. Per EMV specifications[5], two methods can be used by a terminal to build the candidate list: Payment System Environment (PSE) and Explicit Selection.

---

[4] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 1, Section 12

[5] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3 (November 2011), Book 1, Section 12.3

5.1 Payment System Environment (PSE)

Per the EMV specifications, PSE is optional for the chip card's contact interface; it is also optional for the terminal. Because PSE is more efficient than Explicit Selection (described in Section 5.2), an ATM that supports PSE will first send a command to the card to find out if the chip also supports PSE. If the chip does not support PSE, the chip will return a "file not found" response to the terminal. The terminal will then need to use the Explicit Selection method.

If the chip card supports PSE, a certain file will be present in the chip. The chip will return, in a single response, some information about all applications supported by the chip card, including the application name and its associated AID. Optionally, the chip may also send the Application Preferred Name, the Application Priority Indicator (API), Language Preference, and other information for each application it supports.

5.2 Explicit Selection (Also Known as List of AIDs)

If either the terminal or the card does not support PSE, or if PSE is supported but the terminal is unable to find a matching application using PSE, the terminal must use the Explicit Selection method. Per the EMV specifications, all EMV payment cards and payment-accepting terminals must support Explicit Selection.[6]

The terminal will send a command to the card for each of the AIDs the terminal supports, and the card will respond, indicating whether the card supports the AID cited in the command from the terminal. For example, if the terminal supports ten AIDs, ten separate commands are sent to the card and ten responses are returned by the card. Each response indicates whether the chip supports the AID cited in the command. If the AID is supported by the chip, some information about the AID and its associated application is returned; for example, the dedicated file name and application label.

5.3 U.S. Common Debit AID

For guidance regarding AID selection for the U.S. Common Debit AID, please see the ATM Working Committee white paper: "Implementing EMV at the ATM: Requirements and Recommendations for the U.S. ATM Community," section 7.2 – Application Selection.

[6] Ibid.