U.S. Automated Fuel Dispenser Chip Fallback Transaction Processing Best Practices

Version 1.0

Date: June 2020

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.

EMV is a trademark owned by EMVCo LLC.

Table of Contents

1. Introduction

The U.S. Payments 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, in order to provide guidance on fallback transaction processing at automated fuel dispenser (AFD) terminals.

This document clarifies the definition of fallback and provides best practices for supporting fallback transactions and processing magnetic stripe transactions for card programs that are not supported on the contact EMV interface of AFD terminals. Guidance provided in this paper is limited to chip card usage and fallback transaction processing at AFD terminals.

2. What Is a Fallback Transaction?

For the purposes of this document, the term "fallback" is defined as the acceptance of chip cards via magnetic stripe processing at a chip-enabled device. Payment networks require that EMV acceptance devices accept both chip and magnetic stripe cards and thus have both chip and magnetic stripe readers enabled.

When a chip card is inserted, per the relevant payment network specifications, the card information must be obtained via the chip reader and not the magnetic stripe reader if the chip and the chip reader are both functioning. In situations where either the chip or the chip reader is not functioning, it is generally possible to obtain the card information by reading the magnetic stripe. The resulting transaction is referred to as a "fallback" transaction. These transactions are deemed less secure because magnetic stripe acceptance circumvents the control and risk management protection available with chip acceptance.

There are two types of fallback transactions – technical fallback and empty candidate list fallback. The difference between the two types is based on where in the EMV transaction flow it is determined that a chip transaction cannot proceed and that a magnetic stripe transaction may be performed. These two types of fallback conditions are only supported once an EMV acceptance device has been configured to allow fallback.

Fallback transactions are considered a natural part of EMV migration periods; it is considered critical functionality to help with migration to EMV, and important for terminals to support during migration.

2.1 Technical Fallback

Technical fallback is used when a chip-enabled device is unable to read a chip card. In these cases, the chip cannot be accessed at all or successfully read, thus the terminal is not able to obtain sufficient information from the chip. Following this type of technical failure, the card information may be obtained by reading the magnetic stripe. The most common situations where technical fallback may occur include, but are not limited to:

- When the chip on the card is inoperative. No Answer to Reset (ATR) is received from the chip and the magnetic stripe service code states that it is a chip card.
- An invalid ATR is received from the chip.
- The chip reader is malfunctioning.
- In addition, in the early stages of EMV migration it's common to see higher fallback transaction rates due to improper card handling by cardholders (e.g., inserting the card upside down).

2.2 Empty Candidate List Fallback

Empty Candidate List fallback occurs when a terminal is able to successfully communicate with the chip on the card but no matching EMV application is found on the chip. This causes the EMV application selection to fail (i.e., none of the AIDs supported by the EMV acceptance device match any of the AIDs personalized in the chip card). When this occurs, the transaction may be processed by the terminal according to Empty Candidate List transaction processing recommendations as described in Section 4 option 1.

2.3 Fallback-Not-Allowed Scenarios

After successfully completing application selection there are several reasons why a chip transaction may fail and fallback processing is not allowed per payment network security requirements. The following are example situations where fallback processing is not allowed:

- The card is blocked (i.e., disabled by the issuer).
- The chip application is blocked and there are no additional AIDs on the card.
- The transaction is offline declined (Application Authentication Cryptogram (AAC) generated at 1st Generate AC).
- Fallback is not supported by a specific payment network (even if fallback is set globally at the device level).
- The transaction is abnormally terminated (e.g., premature card removal before the transaction has been completed or cancellation of the transaction at any point).

Terminals that have not yet been activated for EMV processing should continue to process magnetic-stripe-read transactions as standard magnetic stripe. Transactions from such terminals should not be marked as fallback since this would misrepresent the terminal entry capabilities and behavior.

Transactions performed using magnetic stripe only cards on EMV-enabled terminals should be marked as magnetic stripe and not as fallback as this would misclassify the transaction and could cause declines. In these scenarios, terminal capability indicators will communicate the terminal's EMV capability to the payment networks and issuers.

Please refer to the U.S. Payments Forum's publication, "EMV Implementation Guidance: Fallback Transactions,"[1] for further details on common problems causing terminals to erroneously identify transactions as fallback and the remedy options.

To help ensure the cardholder is given a full range of options to complete payment at an EMV terminal, overcome initial technical hurdles, and not cause additional cardholder friction, merchants are encouraged to deploy AFD terminals that support EMV fallback processing capability. If fallback transactions are supported, it is critical to properly identify and mark the transactions as fallback.

2.4 Identification of Fallback Transactions

A combination of one or more of the following is used by payment networks and issuers to determine if a transaction is fallback or not: POS entry mode, card service code and terminal entry capability (TEC). Table 1 lists critical values used in the fallback compliance/chargeback process by networks participating in the development of this guidance document.[2]

[1] https://www.uspaymentsforum.org/emv-implementation-guidance-fallback-transactions/

[2] Additional information can be found in the U.S. Payments Forum white paper, "EMV Implementation Guidance: Fallback Transactions," https://www.uspaymentsforum.org/emv-implementation-guidance-fallback-transactions/.

Table 1. Payment Network Requirements: Critical Values in Fallback Process[3]

Critical Values in the Fallback Compliance/Chargeback Process	
Accel	Terminal Entry Capability (TEC); POS Entry Mode; Service Code
AFFN	POS Entry Mode; Service Code; Card Data Input Capabilities
American Express	POS Data Code; Card Service Code
China UnionPay	POS Entry Mode; Terminal Entry Capability; Chip Condition Code
CU24	POS Entry Mode; Service Code
Discover	Terminal Entry Capability (TEC); POS Entry Mode; Card Service Code
MasterCard	Terminal Capability; POS Entry Mode; Service Code; Data Element 55 data components
NYCE	POS Entry Mode; Service Code; Card Data Input Capabilities
PULSE	POS Entry Mode (to identify fallback transactions); Terminal Capability Indicator (to indicate the terminal as being chip-capable for PULSE transactions); Service Code
SHAZAM	Terminal Capability; Input Capability; POS Entry Mode; Service Code
STAR	POS Entry Mode; POS Condition Code
Visa	TEC; POS Entry Mode; Card Service Code; chip data in Data Element 55/Field 55
VOYAGER	Terminal Capability; POS Entry Mode; Service Code; Data Element 55 data components
WEX	Card data input capability, Card data input mode

[3] Contact the payment network or acquirer for specific field/data element references.

3. Unique Considerations for AFD for Fallback

AFD terminals are classified as unattended terminals and are usually subject to different rules and restrictions compared to attended indoor payment terminals.

Some payment networks apply different liability rules governing fallback transactions for POS terminals vs. AFD terminals. Due to liability concerns, fuel merchants may decide to process technical fallback transactions at AFDs for some payment networks while redirecting customers inside to use a POS terminal for other networks.

AFD terminals usually support fleet prompting for open and closed loop fleet card programs. Fleet prompting information may be found on the magnetic stripe of the card as well as on the chip. As proprietary data elements and formats are used by different fleet payment networks, fleet-supporting AFDs should refer to all supported fleet payment networks for their program specifics.

AFD terminals differ from POS terminals in that they are usually "combined" readers, meaning the magnetic stripe reader and chip reader are contained in the same slot. This particularly can impact technical fallback processing.

When a consumer inserts a chip card into an AFD terminal, the card's presence is detected both mechanically and electronically. Unlike a POS terminal that receives a generic "chip error," an AFD can experience multiple instances of "chip errors."

If a magnetic stripe card is used:

- No ATR received. This is a common use case for loyalty, fleet, and some other non-branded payment cards. The magnetic stripe is read as the card is removed and the transaction is processed as a magnetic stripe transaction. This is not considered a fallback transaction.

If a chip card is used:

- No ATR received. Unlike POS terminals that respond with "Chip Error" when a chip is not electronically detected (no ATR), at AFD terminals this simply becomes a magnetic stripe read and the track data is read as the card is extracted. It is then up to the payment application to decide how to handle the magnetic stripe data which indicates whether the card is a chip card and if this should be treated as a chip error. At a POS terminal, the application would instruct the cardholder to insert the card. If the chip is truly malfunctioning, the card may not be used, or a technical fallback could be applied. If the transaction is processed, it will be sent as a technical fallback transaction.
- An ATR is received, but the chip cannot be read. This can be handled as a traditional technical fallback since the chip transaction has begun and the chip has returned a chip error.
- An AFD terminal's combined chip/magnetic stripe reader would handle Empty Candidate List processing in the same way as a POS terminal.

4. Payment Network Policies for AFD Technical Fallback

The current published policies made available by each payment network related to AFD technical fallback have been summarized in Table 2. For any questions regarding these policies, it is recommended that merchants contact their acquirer for additional information.

Table 2. Payment Network Technical Fallback Policies

Payment Network	Technical Fallback
American Express	• Refer to American Express Automated Fuel Dispenser Guide U.S. Region, March 2020, section 4.4. "Fallback from an AEIPS or Expresspay Transaction to Magnetic Stripe shall not be possible at an AEIPS/Expresspay enabled AFD."

China UnionPay (CUP)	• For Discover acquired:
	  ○ Technical fallback transactions must specify a Point of Sale Entry Mode (PEM) of 85. (Note: this is specific to Discover processing for all U.S.-based transactions that are acquired by Discover.)
	  ○ Issuer is liable for approved fallback transactions. (EMV counterfeit and lost-and-stolen liability is not applicable to fallback transactions.)
	• For CUP direct-acquired:
	  ○ Technical fallback transactions must specify a Point of Sale Entry Mode (PEM) of 02 or 90, Terminal Entry Capability of 5 or 6, and Chip Condition Code of 2. The combined value features the fallback transaction.
	  ○ Issuer is liable for approved fallback transactions. (EMV counterfeit and lost-and-stolen liability is not applicable to fallback transactions.)

Discover	• Technical fallback transactions must specify a Point of Sale Entry Mode (PEM) of 85. • Issuer is liable for approved fallback transactions. (EMV counterfeit and lost-and-stolen liability is not applicable to fallback transactions.)
JCB	• Technical fallback transactions must specify a Point of Sale Entry Mode (PEM) of 85 (Note: this is specific to Discover processing for all U.S.-based transactions that are acquired by Discover.) • Issuer is liable for approved fallback transactions. (EMV counterfeit and lost-and-stolen liability is not applicable to fallback transactions.)
Mastercard	• Technical fallback transactions should be processed with proper indication of fallback transaction. Properly marked fallback transactions are the issuer's liability (from chip counterfeit and lost-and-stolen chip liability shift rules perspective) for both indoor and AFD terminals.
NYCE Payment Network	• Technical fallback should be supported at the terminal and be processed with the Point of Sale Entry Mode (PEM) of 80. • Issuer is liable for approved fallback transactions.
PULSE	• Technical fallback transactions must specify a Point of Service Entry Mode (PEM) of 80. • Issuer is liable for approved fallback transactions.
Visa	• Fallback must be supported at the site in order to honor acceptance of all Visa cards. • For fallback transactions processed outside at the AFD, the merchant will retain lost-and-stolen fraud liability. (However, there is a reverse lost/stolen liability shift for chip-on-chip transactions.) Fallback can also be moved inside the fuel site store where issuers will be responsible for lost-and-stolen fraud liability for fallback transactions.
VOYAGER	• The merchant will retain fraud liability for fallback transactions at the AFD.
WEX	• The merchant will retain fraud liability for fallback transactions at the AFD.

5. Options for Processing Empty Candidate List Scenarios: Processing of Fleet Card Programs Not Supported on EMV Interface

AFD terminals support a variety of payment products, including credit, debit, fleet, gift, and loyalty cards. These payment products may not all convert to EMV chip technology at the same time. Specifically, scenarios can occur when the terminal is only enabled for certain EMV payment products but not yet for all magnetic stripe supported payment products, such as fleet payment products, for a certain terminal. In such a case, when the fleet payment network's EMV card is inserted into the terminal, the terminal could end up with an Empty Candidate List since the fleet payment network's EMV AID has not been certified and deployed to the terminal.

To avoid such issues, terminals should enforce EMV processing rules only for the card payment products and associated AIDs they support through the EMV interface.

Note: Empty Candidate List scenarios are possible in other merchant categories and for other payment network cards that are not supported for EMV; however, this section focuses on AFD and fleet card processing only.

Below are possible solutions for AFD systems to handle the fleet payment product AIDs that are not supported by a terminal for EMV. Merchants should consult their acquirers and terminal vendors to determine which option is feasible.

5.1 Option 1[4]

If the merchant accepts a fleet-issued card, but the terminal is not yet coded or certified to process EMV transactions for that fleet card (including AID and process flows), in order to minimize disruption to the cardholder, all transactions for that fleet card should be processed as magnetic stripe transactions (using the Empty Candidate List fallback).

The merchant's terminal vendor should build logic that identifies that the transaction is an Empty Candidate List fallback, uses the BIN to identify the payment network, and decides the processing parameters based on card payment network/issuer guidance.

It may not always be possible to apply the above-mentioned BIN logic and processing parameters, controls and decisions at the terminal level. These controls and decisions may be made at the electronic payment server (EPS), merchant payment switch/gateway or the acquirer level. In order to avoid misclassifying the transaction, it is critical that these decisions are made prior to sending the transactions to the respective network.

The following process is an example that may be followed to ensure proper processing of such transactions:

1. The EMV card is inserted and the terminal starts EMV processing.
2. The terminal cannot find a matching AID on the card (results in an Empty Candidate List).
3. The terminal will go into fallback and will allow the magnetic stripe of the card to be read while ignoring the service code so that the card is not requested to be entered again.

[4] There may be some variations in this approach. Consult with the solution provider and acquirer about how to accept transactions.

4. Once the magnetic stripe track data has been extracted, it is up to the solution to decide where the BIN read from the magnetic stripe will be compared to the payment networks accepted by the terminal.
    - If the BIN is identified as one from a payment network that is supported on the EMV interface, the transaction should be processed as fallback or terminated based on corresponding network rules. (Necessary indications should be made in the authorization message if the transaction is processed.) See Table 3 for payment network details.
    - If the BIN is identified as one from a payment network that is not supported on the EMV interface but supported only as magnetic stripe, the transaction should be processed as a regular magnetic stripe transaction, while indicating that the terminal is not enabled for EMV for that payment network based on the corresponding payment network rules. (This is not a fallback transaction from the payment network perspective.) How terminals send the transaction to the acquirer may vary; in some cases, the transaction may be sent to the acquirer as technical fallback.
    - If the BIN is identified as not recognized, the transaction should be terminated.

The above solution addresses the issues of processing all Empty Candidate List scenarios and provides a consistent approach that can be used across the industry.

For further details on proper identification of fallback and/or magnetic stripe transactions and terminals, please refer to individual network specifications. The current published policies made available by each payment network related to Empty Candidate List fallback have been summarized in Table 3.

Table 3. Payment Network Considerations on ECL Fallback Implementation/Liability Shifts

Payment Network	ECL Fallback Implementation/ Liability Shift Considerations
American Express	• Refer to American Express Automated Fuel Dispenser Guide U.S. Region, March 2020, section 4.4. "Fallback from an AEIPS or Expresspay Transaction to Magnetic Stripe shall not be possible at an AEIPS/Expresspay enabled AFD."
China Union Pay	• Empty Candidate List transactions must specify a Point of Sale Entry Mode (PEM) of 02 (magnetic stripe). • Prior to April 2021, the Discover EMV Fraud Liability Shift does not apply to ECL Transactions. Effective April 2021, issuers will be able to dispute Empty Candidate List transactions using the EMV FLS Dispute Reason Code. • Note: The above statement is applicable only to Discover acquired transactions.
Discover	• Empty Candidate List transactions must specify a Point of Sale Entry Mode (PEM) of 02 (magnetic stripe). • Prior to April 2021, the Discover EMV Fraud Liability Shift does not apply to ECL Transactions. Effective April 2021, issuers will be able to dispute Empty Candidate List transactions using the EMV FLS Dispute Reason Code.
JCB	• Empty Candidate List transactions must specify a Point of Sale Entry Mode (PEM) of 02 (magnetic stripe). • Prior to April 2021, the Discover EMV Fraud Liability Shift does not apply to ECL Transactions. Effective April 2021, issuers will be able to dispute Empty Candidate List transactions using the EMV FLS Dispute Reason Code.
Mastercard	• Empty Candidate List cases must be terminated. No transaction should be generated as magnetic stripe or fallback when the Empty Candidate List scenario exists.

Payment Network	ECL Fallback Implementation/ Liability Shift Considerations
NYCE	• Empty Candidate List transactions must specify a Point of Sale Entry Mode (PEM) of 02 (magnetic stripe). • Merchants are liable for disputed Empty Candidate List transactions.
PULSE	• Empty Candidate List transactions not eligible for fallback Point of Service Entry Mode value of 80, merchant must specify a Point of Service Entry Mode value of 02 (magnetic stripe). • Merchants are liable for disputed Empty Candidate List transactions.
Visa	• If the card has a Visa BIN and Empty Candidate List, the merchant can decline at the POS. • Fallback can be moved inside the fuel site store as there is a different liability inside for lost-and-stolen. On magnetic stripe transactions outside at the AFD, the merchant retains liability for lost-and-stolen fraud on a magnetic stripe card. (There is a reverse lost/stolen liability shift for chip-on-chip transactions.)
VOYAGER	• Empty Candidate List transactions must specify a Point of Sale Entry Mode (PEM) of 02 (magnetic stripe).
WEX	• Empty Candidate List transactions must specify a card data input mode of 2 (magnetic stripe read).

5.2 Option 2

An alternative way of avoiding Empty Candidate List cases from known fleet programs could be to have AFD terminals preloaded with all possible future supported fleet AIDs, and pass EMV data to the acquirer systems for all transactions regardless of certification status.

In order for this option to work, merchants, acquirers and fleet card issuers would need to agree on the merchant's passing EMV data to the acquirer regardless of the terminal's certification or readiness status.

In addition, acquirer systems would need to be ready to process EMV transactions for all relevant fleet cards, or have mechanisms to stop these transactions as needed.

Note that this option may not be supported by terminal vendors. Merchants should consult their acquirers and terminal vendors to determine if this option is feasible.

6. Legal Notice

The information in this document is intended to describe identified and potential solutions to avoid complications due to fallback in AFD transaction processing, as a convenience to interested stakeholder. It is not intended to and does not constitute legal or technical advice, and should not be relied on for any such purpose. All warranties of any kind, whether express or implied, are hereby disclaimed, including but not limited to the implied warranty of fitness for a particular purpose. Any person that uses or otherwise relies on the information set forth herein does so at his or her sole risk.

This document is not intended to be exhaustive. AFD implementations and circumstances may differ, applicable rules, processing, liabilities, obligations and/or results may impact or be impacted by specific facts or circumstances, and each payment network determines its own rules, requirements, policies and procedures, all of which are subject to change. Accordingly, AFD owners and operators, and others implementing EMV chip technology in the U.S., are strongly encouraged to consult with the relevant payment networks, acquirers, processors, vendors and other stakeholders prior to implementation.