EMV Fallback Transactions

WHITE PAPER

March 2017

EMV introduces new technology and new terminology, as well as transaction scenarios that simply did not occur in a magnetic stripe–only world. One of these new scenarios is fallback. In this white paper, we will define fallback and give examples of how fallback can occur. We will also provide recommendations for terminal owners, acquirers, and issuers so they can take steps to reduce the incidence of fallback, and recognize it when it does occur.

Be There. Be More.

CO-OP FINANCIAL SERVICES

Contents

White Paper

What is Fallback?

The actual term is 'technical fallback,' but it's commonly referred to as simply fallback. Fallback can occur when a chip card is presented to a terminal that is EMV-enabled, that is, the terminal is able to process an EMV transaction, but for some reason the chip on the card is not read, so a magnetic stripe transaction is generated instead of an EMV transaction.

Let's look at how this can happen.

Determining the Card Technology

How does the terminal know that a chip card is being presented? In many cases, the terminal will be configured to read the magnetic stripe on the card before attempting to read the chip. This is particularly true in regions where there are still a lot of cards in that market that only have a magnetic stripe on them. There's no need to try to read the chip first, if there is a good chance the card that is being presented is not a chip card.

The terminal will check the service code in the magnetic stripe to see whether the card was created as a magnetic stripe card or as a chip card. This can be determined by interrogating the first digit of the three-digit service code. The diagram below shows the general format of the Track 2 data.

;	Primary Account Number	=	Expiration Date	Service Code	Discretionary Data

The service code follows the expiration date in the track 2 data. Generally, a service code starting with 1 indicates a magnetic stripe card, and a service code starting with 2 indicates a chip card. There are other possible values, but these are the most common ones.

If the service code on the card indicates that the card is a chip card, the EMV-enabled terminal will attempt to communicate with the chip on the card. If for some reason this communication fails, the terminal will typically be configured to generate a magnetic stripe transaction. At the POS, this usually means that the cardholder is prompted to swipe their card so that the magnetic stripe can be read.

Optionally, the terminal could reject the card, in other words, present a message on the screen telling the customer that their card could not be accepted, but this is not very customer-friendly. Therefore, most terminal owners will configure the terminal to generate a magnetic stripe transaction in this situation. This is a fallback transaction; the chip in the card could not be read, so the terminal had to *fall back* to the less secure magnetic stripe technology in order to proceed with the transaction.

Fallback is only relevant when the card is physically present at the terminal, so it is not relevant for card-not-present transactions. And, in order to generate a fallback transaction, the terminal must have the ability to read the magnetic stripe.

Fallback Resulting from Criminal Intent

A common form of criminal activity is skimming, where a criminal captures the data from the magnetic stripe of a legitimate card, usually without the cardholder's knowledge. The criminal then encodes that track data on a different card, and uses that cloned, or counterfeit, card to obtain cash or merchandise. When the issuer receives the authorization request they cannot tell whether a real card was used, or a counterfeit card was used, by looking only at the track data, because the data in the mag stripe is exactly the same on both cards.

There are several scenarios where fallback can indicate criminal activity related to skimming.

With the fraud scenario previously mentioned, the criminal skims the track 2 from a legitimate chip card, and puts the unaltered track 2 data on another card, often a blank white plastic card. The service code in the track 2 indicates it's a chip card, but there is no chip on the counterfeit card, so when this card is used at an EMV-enabled terminal, a fallback transaction is generated.

In another scenario, the criminal takes this a step further. The criminal skims the track 2 from a legitimate chip card, and puts the data on a blank white plastic card. Then they take the additional step of putting a decal or something on the face of the card to make it look like there is a chip on the card, even though there is no real chip on the card. This might be done in an attempt to fool a sales associate. Of course the EMV-enabled terminal cannot obtain data from the fake chip, so a fallback transaction is generated.

A criminal can also skim the track 2 from a legitimate chip card, change the service code to indicate the card is mag stripe not chip, then put the modified data on a blank white plastic card. They might try this to try to trick the issuer's authorization system into believing that the transaction was initiated by a mag stripe card and is therefore not fallback. However, the issuer may have a record of the original service code for the card, and if comparing the service code in the authorization request to the service code that was actually assigned to the card is part of the authorization process, then the authorization system will recognize that something is wrong. Even if this comparison is not done during authorization, the service code is part of the card security code calculation; if the issuer is doing their due diligence during the authorization process, they should validate the card validation code, such as the CVV, that is part of the track data and is therefore sent in a mag stripe transaction. This validation will fail if the service code has been altered. It is important to note that the chip also contains a card security code value, but for security reasons, the card security code result for the chip is different from the card security code result for the magnetic stripe.

There are other ways that someone can intentionally cause fallback to occur. The chip can be covered with tape or clear nail polish, so that from a distance, it's impossible to tell that there is anything wrong with the chip card. The chip can be intentionally damaged. The chip can even be removed from the card altogether.

Criminals are also exploiting the "empty candidate list" scenario. A chip card is presented at an EMV-enabled terminal. The mag stripe on the card contains data that was skimmed from a legitimate card. The applications on the chip card, and their representative AIDs (Application Identifiers), do not match any AIDs that the terminal supports, so an EMV transaction cannot be generated. The criminal swipes the card, and a fallback transaction is generated based on the data in the mag stripe, which was skimmed from a legitimate card.

Another possible fraudulent scenario is if a retail associate can find a workaround process to trigger a magnetic stripe transaction when a chip card was actually presented at an EMV-enabled terminal.

Fallback Resulting from Non-Criminal Intent

Fallback is not, however, always the result of criminal activity. Here are some scenarios where fallback can occur in non-fraudulent situations.

A legitimate cardholder may have a chip card where the chip has been damaged unintentionally. Maybe it was inadvertently cut with a sharp instrument, or was marked over with a crayon. A customer might have scratched the chip, thinking the chip card was a new form of scratch-off lottery ticket. A cardholder might deliberately remove the chip from their card; not with the intent to perpetrate fraud, but because they do not understand the purpose of the chip.

In each of these scenarios, when the card is inserted into the terminal, the service code in the magnetic stripe will indicate that this is a chip card, but the terminal will not be able to communicate with the chip.

"Implementation fallback" refers to the scenario where the acquirer or merchant has a high rate of fallback transactions due to a hardware or software issue. Information in the transaction indicates that the terminal is EMV-enabled when actually it is not. This can happen in the early stages of an EMV migration and is usually due to a lack of understanding on the part of the terminal owner, acquirer or merchant as to how to configure their terminals and how to set the terminal entry capability field in the authorization request. Setting the terminal entry capability incorrectly is the most common cause of apparent fallback in the US.

There could be other configuration errors in the terminal.

Chip card readers do get dirty. They can accumulate dust, or get gummed up by the residue of adhesive that was used to affix the peel-off activation sticker to the face of the card. The contacts in the chip card reader therefore cannot make good contact with the chip on the card, so the chip cannot be read. In this case, there is nothing wrong with the chip card at all.

There could be an error in the transaction path. As a transaction makes its way from the terminal to the acquirer to a network to the issuer, the message format may change, and if all parties are not careful, or some parties do not yet support EMV, data may get lost as it is passed from one format to another. The issuer may then receive incorrect, invalid, or ambiguous information in the request, causing the issuer to interpret the transaction as fallback, when actually the transaction may have started out as a good EMV transaction at the terminal.

The cardholder might insert the card incorrectly, or swipe it multiple times. Some of the card brands recommend that the terminal attempt to read the chip 2 or 3 times before falling back to magnetic stripe.

In each of these cases, a legitimate chip card was used by the rightful cardholder, but a fallback transaction resulted.

As long as payment cards continue to have a magnetic stripe, the magnetic stripe data can be skimmed from the card. There are no plans at this time to remove the magnetic stripe from US-issued chip cards, although other countries may be doing this.

Terminal Owner and Acquirer Best Practices

There are several things that terminal owners and acquirers can do to reduce the number of fallback transactions their terminals might generate.

Be There. Be More.

CO-OP FINANCIAL SERVICES

First and foremost, it is critical to ensure data integrity in online transactions. An EMV transaction contains more information than a mag stripe transaction, and it is essential to put the right values in the right fields so the issuer can get as accurate a picture as possible of what happened at the terminal.

An authorization request may include a field that specifies the terminal entry capability. This indicates the highest technology the terminal is capable of handling: can it only handle mag stripe transactions, or can it process EMV transactions? Just because you have a chip card reader in your terminal, this does not mean you can automatically set this field to indicate that the terminal is capable of processing EMV transactions! The terminal entry capability must reflect not only the highest level of capability supported by the terminal hardware, but also by the terminal software.

Even though a terminal may be capable of processing EMV transactions in many circumstances, this does not mean that the terminal can successfully generate an EMV transaction every time a chip card is presented. Within the authorization request, there is typically a field where the acquirer can indicate how the data was actually obtained from the card: was the mag stripe read, or was the chip read. This field is often called the POS Entry Mode. It's very important to set this value correctly in the transaction request.

Some message formats contain a field where the acquirer can set a specific value that indicates the transaction is definitely fallback. CO-OP puts the correct value in this field in online transaction requests that members receive from us. More information about this scenario is included later in this white paper.

It's also important to keep the software in the terminal up to date. The terminal will contain special EMV software, known as the kernel. This software kernel has an expiration date, so it will eventually require re-certification or replacement. Running an old version of EMV software may mean that your software is not able to handle certain unusual scenarios it may be presented with, in the manner recommended by the card brands.

In addition to having correct software, and up-to-date software, in place, the terminal must also be configured with the correct list of AIDs that the terminal supports.

It's important to keep the chip card reader clean. Many ATM owners clean the chip card reader as part of their regular ATM maintenance procedures.

There may be a rare situation where the chip cannot be read, but instead of swiping the card, the sales associate goes straight to manual, key entry of the transaction. The card brands strongly discourage this approach. The chance of both the chip and the mag stripe on the card being bad is extremely low, so if the chip cannot be read, the mag stripe should be swiped. Swipe is much more secure than manual key entry, and provides more information for the issuer to evaluate in the transaction during the authorization process.

Issuer Best Practices

Here are some good practices issuers can follow to reduce the risk associated with counterfeit card fraud.

When authorizing a mag stripe transaction, that is, a transaction that does not contain EMV data, whether the transaction is fallback or not, be sure to validate the card security code, such as the CVV, in the track data. If the criminal has changed the service code, the card security code validation will fail.

When authorizing a transaction, if you do receive EMV data, be sure to validate the Authorization Request Cryptogram (ARQC). This is the primary way for the issuer to ensure that the card that was used to initiate the transaction is legitimate. If you have gone to all the effort, time, and expense of issuing chip cards, then by not validating the ARQC, you have basically negated your investment.

As previously noted, the card security code in the mag stripe will be different from the card security code in the chip, which is sometimes called the iCVV (using Visa terminology). If you receive a legitimate EMV transaction, with an ARQC, and you confirm that the ARQC is valid, there is no need to also validate the iCVV; this is overkill.

It's essential that you do not abandon the rules and logic you currently use to assess risk when authorizing a transaction. Things you are already checking with mag stripe transactions will continue to be important for you to check with EMV transactions, for example:

- An indication that the card was reported as lost or stolen
- The amount, location, and Merchant Category Code of the transaction
- Velocity of transactions performed by this card
- Any risk score that might be calculated for the transaction

You will also want to factor in any new fraud trends related to EMV. CO-OP is monitoring trends across all risk clients for this very purpose but we welcome and encourage our credit unions to collaborate by reporting new fraud trends as they are affecting your card portfolios.

Each issuer will have their own level of risk tolerance. It's not "one size fits all." What works well for one organization may not be appropriate for another organization. It's important to strike a balance, and avoid extremes when deciding how to handle fallback transactions. You will want to avoid the following extremes:

- Decline everything that remotely resembles fallback or counterfeit card fraud, to avoid any possibility of liability
- Approve everything that might potentially be fallback, because the percentage of potential fraudulent transactions is small, or because of fear of declining a VIP transaction

Balancing risk management with maintaining a positive cardholder experience is paramount, especially in the early stages of an EMV implementation.

Identifying Fallback Transactions Utilizing CO-OP Resources

In the online messages that CO-OP sends to credit unions' core processors, fallback transactions will have one of two unique values in Data Element 22, which is the POS Entry Mode. Potentially the core processor can log this information, and report on it for the credit union. These values are:

- 79: indicates fallback, where the card number was entered manually
- 80: indicates fallback, where the card number was obtained from track data in the magnetic stripe

Data Navigator

When using Data Navigator, on the Transaction Search screen, the Card Input Mode field is towards the bottom of the screen. Click on the "List" link to pull up a list of available values. The values related to fallback are: B (which equates to POS Entry Mode 79), and C (which equates to POS Entry Mode 80).

CO-OP Revelation

When using CO-OP Revelation®, there is an existing Transaction Filter called "Fallback EMV Transactions" that Level 2 and Level 3 subscribers can use in a transaction search. It will return only those transactions that had a POS Entry Mode of 79 or 80. The POS Entry Mode is captured in the field in Revelation called the "Card Entry Method."

A user could also create their own Transaction Filter using the Card Entry Method and any additional data elements.

Fight Fraud with Aggressive Fraud Tools

CO-OP presently monitors for excessive fallback activity using our neural net fraud prevention tool. During the Spring of 2017 CO-OP will be introducing a new fraud tool called "Fraud Navigator." Fraud Navigator will enable CO-OP to limit fallback transactions for credit unions that wish to develop some additional fraud strategy that will ease the concerns associated with fallbacks that are not controlled today by routine fraud monitoring practices. CO-OP will post more information and the latest updates on Fraud Navigator as the information becomes available. Please visit our website CO-OPfs.org to download our latest security eBook.

Additional Best Practices

When interrogating the data in a message format where there are no specific values that indicate that the transaction was definitely fallback, it is still possible to make that determination. If the service code in the track data indicates that the card is a chip card, and the terminal entry capability indicates that the terminal can process EMV transactions, but there is no ARQC in the request, and the POS Entry Mode indicates that data was obtained by reading the mag stripe, not the chip, you are probably looking at a fallback transaction.

Even though there are ways to detect that a transaction is fallback, unfortunately there is usually nothing in the authorization request that clearly indicates exactly WHY a fallback transaction was generated. As a result, it is extremely difficult, and often impossible, for an authorization system to tell the difference between fallback that was caused by criminal intent, and fallback that was caused through cardholder ignorance, bad terminal configuration, or other events that occurred during transaction processing. This is why some issuers will simply decline all fallback transactions across the board.

Additional Recommendations

It's important to familiarize yourself with the various payment network rules and regulations for "excessive" fallback, and any associated compliance actions or penalties.

CO-OP's risk department can assist credit unions that wish to develop fraud strategy around EMV fallbacks. CO-OP is already deploying global fraud strategy today to curtail these transactions. Credit Unions that require additional support for fraud that is a direct result of EMV fallbacks

Be There. Be More.

CO-OP FINANCIAL SERVICES

should immediately contact CO-OP's risk team via email at RiskEscalation@CO-OPfs.org.

Monitor your transaction activity. This may include developing new reports, or modifying existing reports, to recognize fallback and provide data about fallback transactions to interested parties.

Terminal owners should periodically check device logs; look for unusual and intermittent errors. Look for patterns related to fallback. Is fallback always occurring with the same card, no matter where it is used? Or with all cards in a given BIN? Is there a higher incidence of fallback at one particular terminal? Or at terminals that are manned by the same sales associate? Do you see a lot of fallback from a particular retailer? Or from a specific ATM?

If you detect a pattern, contact the retailer, issuer, or ATM owner. They may not even be aware of a problem. Sometimes the only way to solve a problem is to reach out to someone at another organization and work together to reduce fraud.

You should also become familiar with your authorization and decline rates before EMV implementation, so you can spot trends as you migrate to EMV, and see if new trends develop after your migration is complete.

Global Statistics Related to Fallback

When a region is migrating to EMV, fallback rates may start around 7 to 10 percent, but this percentage should quickly drop as implementation issues and data integrity issues are corrected, and as issuers refine their chip card profiles and their authorization logic. Visa and MasterCard expect a 2 percent or lower fallback rate in the US.

Globally, fallback rates are around 1 percent or less of total transactions. This is because there are many mature EMV markets around the world, and some countries no longer allow fallback at all. In these mature EMV markets, if a terminal cannot read the chip, the transaction cannot proceed. At this time there are no plans to disallow fallback with US-issued cards at US terminals, given the amount of terminals that still need to be upgraded to EMV in the US.

Resources and References

Here are some sites where you can find publicly available documents that are excellent sources of information.

- CO-OP Financial Services offers a variety of on-demand educational opportunities and subject matter, including expert-led educational webinars.
  For a list of available opportunities please visit http://CO-OPfs.org/insights/training.
- The US Payments Forum (formerly known as the EMV Migration Forum) has many free white papers, videos, and recorded webinars available on their website.
- Consumer-friendly, easy-to-understand information can be found at gochipcard.com. Information is geared specifically to consumers and the information is complimentary.

Summary

EMV introduces new technology and terminology. Fallback is just one aspect of EMV you should become familiar with. Fallback transactions can be regarded by some issuers as high-risk transactions because they represent potential for loss. Please carefully evaluate your credit union's volume of legitimate to fraudulent EMV fallbacks to ensure that you are not jeopardizing non-interest income with unnecessary transactional denials.

Please keep in mind that as long as a card has a magnetic stripe on it there is a chance for that data to be skimmed and used for fraudulent purposes. Therefore, we must constantly be alert to criminal activity related to fallback and we encourage CO-OP credit union clients to collaborate as needed to ensure that we are meeting the needs of your business and maximizing your member's experience with seamless and secure transactions.

Special thanks are extended to CO-OP's Technology Committee for providing comments and guidance during the publication of this document.

03222017CF17190

Be There. Be More.

CO-OP FINANCIAL SERVICES