VISA smart

Fallback Guidelines
Asia Pacific Region
September 2004

VISA

Table of Contents

1. Document overview

1.1 Audience

The intended readers are Visa members that are implementing VSDC programs and Visa internal staff. This document will help both Visa issuers and Visa acquirers to understand what guidelines to follow when sending and receiving a fallback transaction.

The Technical appendix can be handed out to vendors for correct implementation.

1.2 Reference

Document Reference	Document Full Title, Publication Date, Version
VIS	Visa Integrated Circuit Card Specification, Application Overview, Terminal Specification, Card Specification, 31 October 2001
EMV 2000	EMV 2000 Integrated Circuit Card Specifications for Payment Systems – Version 4.0, Books 1-4
MIG Issuers	VSDC Member Implementation Guide for Issuers, version 3.0, July 2003
MIG Acquirers	VSDC Member Implementation Guide for Acquirers, version 3.0, July 2003
CAD	Chip Card Acceptance Device Reference Guide, Requirements and Best Practices, Version 6.0, July 2003
VIOR	Visa International Operating Regulations
APROR	Asia Pacific Regional Operating Regulation

1.3 Terminology and Definitions

Term	Definition
AAC	Application Authentication Cryptogram
ATM	Automated Teller Machine
ATR	Answer to Reset
CVM	Cardholder Verification Method
HiCo	High Coercivity
LRC	Longitudinal Redundancy Check
PIN	Personal Identification Number
PKE	Pan Key Entry
POS	Point of Sale Terminal
SMS	Single Message System for Authorizations
TMS	Terminal Management System
UAT	Unattended Device
V.I.P System	VisaNet Integrated Payment System. The Online processing component of VisaNet
VIOR	Visa International Operating Regulations
VSDC	Visa Smart Debit Credit

1.4 Scope

This document is the Visa Asia Pacific Region's guide to issuers, acquirers and merchants on the best practices of processing transactions that fallback from chip to magnetic stripe. Some of the principles described here are incorporated into the *Visa International Operating Regulations* (*VIOR*) and as such are mandatory across all countries and merchant relationships and some of the principles will be incorporated into the *Asia-Pacific Regional Operating Regulations (APROR)*; in other cases the guidance is a recommendation. In this document mandatory requirements are indicated by the word "**must**" and recommendations by "**should**" or "**may**".

In some cases specific agreements may be made by members at the national level, and will apply within that country according to terms agreed between the members making the agreement.

Throughout this document "chip card" and "chip" should be taken to mean an EMV- and VIS-Compliant Chip Card, and "chip terminal" means an EMV-certified terminal[1] enabled and configured for chip card acceptance.

The guidance takes into account the *VIOR* to ensure international compatibility in relation to chargebacks and liability

This paper is limited to technology fallback transactions where the primary technology (chip or magnetic stripe) supported by **both card and terminal** cannot be used. Cardholder Verification Method (CVM) fallback is excluded.

[1] Face-to-face, unattended or ATM

2. Background

The *VIOR, Volume I* defines that all Chip Reading Devices on or after 1 April 2002, must be capable of requiring an online authorization for the next consecutive magnetic stripe read transaction originated from a chip card when a chip transaction could not be performed. This means that all activated chip terminals today must be able to handle a fallback transaction. For the issuer to be able to interpret if the incoming authorization due to fallback, the right fields have to be populated by the acquirer.

2.1 Global View

Since EMV migration is proceeding in different paces within Visa's six different regions, so far only the EU region has defined in their Operating Regulations what an acquirer must send in the authorization to not be liable for any fraudulent transaction that was performed in a fallback mode.

VIOR, Volume I currently has a principle stating that if a chip transaction fails, the next consecutive transaction at the same terminal, when the magnetic stripe is read, has to go online. However since no chargeback rules are defined, an issuer cannot charge back an inter-regional fallback transaction that was not correctly populated.
The Member Implementation Guides for Issuers and Acquirers define what fields to populate for a fallback transaction as Best Practice.

In line with the commencing liability shift, to protect intra-regional members, the *APROR* will be updated to support fallback chargebacks, see paragraph 4 for more details.

2.2 Allowing fallback transactions

The main reason for allowing fallback transactions is to support a technology migration from magnetic stripe to chip. As with all new technologies, there can be interoperability issues or other problems making the chip card or the chip terminal not function to its fullest. During this rollout period when new chip cards and chip terminals reach the markets, a grace period allowing falling back from chip to magnetic stripe will support the concept of 'honor all cards'. However, since this is mainly allowed due to new technology, when a market or a region has reached a certain maturity point, fallback transactions should be disallowed. The maturity point could be regarded as when reported interoperability issues are down to a minimum or when fallback transactions are between 2 and 3 percent.

It is always up to the issuer's discretion to decline any fallback transaction on transaction-by-transaction basis and as a business decision. By a certain point, an issuer can decline all fallback transactions before any national or regional mandates forbid fallback transactions.

3. Fallback

3.1 Definition of fallback

A fallback transaction is one in which the primary technology of the card and terminal is not used (i.e. one that would be expected by both issuer and acquirer for a particular card and terminal). In some countries and in other regions, this will include both technology fallback and Cardholder Verification Method (CVM) fallback (where the preferred CVM cannot be used), however this paper considers only technology fallback.

A technology fallback transaction would be a transaction from cards and terminals that are chip enabled; is processed as a magnetic stripe transaction alternatively when the card and terminal is magnetic stripe enabled; and is processed as a manual (paper) transaction. In other regions, it may also include PAN Key-Entered (PKE) transactions where the PAN and expiry date are entered manually into an electronic terminal.

3.2 Supporting documentation

According to *VIOR, Volume I, rules 4.4.C.2.e – second bullet, 4.4.C.2.f and 5.2.E.3 – last bullet*, after a chip read failure, the terminal must allow a magnetic stripe reading of the chip card, and send the transaction online to the issuer. In the event that online authorization capability is not available, the merchant may be given the option to perform voice authorization to complete the transaction.

VSDC Member Implementation Guide for Acquirers and *VSDC Member Implementation Guide for Issuers* define a fallback transaction and the data that must be populated in the respective fields.

3.3 Chargeback rights

Data fields mentioned in both Member Implementation Guides are currently optional. However acquirers are strongly encouraged to populate the right fields to inform the issuer that a fallback transaction has taken place. *VIOR, Volume I*, does not contain a definition of a fallback transaction and there are no chargeback rules to support the issuer in the right to receive full information in the authorization indicating a fallback transaction. *VIOR, Volume I* does however say in 4.4.C.2.f (May 2004 version) that all chip terminals must send to the issuer the next magnetic stripe read transaction originated from chip cards online when the last chip reading failed. This will however change for intra-regional transactions with the fallback liability shift (See paragraph 4).

4. New Asia Pacific Operating Principles

4.1 Correctly completed fallback transactions

For correctly completed fallback transactions (as defined in the Technical appendix and in the Member Implementation Guides), where the appropriate values identifying the transaction as a fallback transaction are included in the authorization message, the issuer's chargeback rights are limited to disputes concerning the goods and services supplied. This includes fallback transactions performed with PIN.

4.2 Incorrectly completed fallback transactions

The transaction is at the liability of the acquirer if the transaction is a fallback transaction (as defined in paragraph 3) and either of the following conditions applies:

- The transaction is not authorized by the issuer or the issuer's agent
- The appropriate values identifying the transaction as a fallback transaction are not included in the authorization message (or the transaction is not clearly identified as a fallback transaction in a voice authorization request).

4.3 Asia Pacific Regional Operating Regulations

Asia Pacific Regional Operating Regulations will be updated in May 2005 edition to reflect the new rules regarding intra-regional fallback liability shift, effective from 1 January 2006.

5. Merchant perspective

5.1 Merchant risk exposure

The rate of fraud on fallback transactions is higher than that on chip transactions; this is because the chip may have been damaged deliberately in order to invalidate the security checks, and there would be more scope for cashier fraud, skimming and transaction replay. Merchants must be aware that the likelihood of a decline or referral response is higher for fallback transactions than when the chip data is present.

Merchants with chip card terminals are therefore advised to ensure that wherever possible chip cards are processed using the chip. Merchants who carry out chip transactions are automatically protected against counterfeit chargebacks.

5.2 Minimizing fallback rates

A fallback transaction takes place when the chip terminal is unable to complete a transaction with the chip on the card. This may be because either the card or the terminal is faulty. In practice, the reliability of chip cards is very high, and provided terminals are kept clean and the contacts are not damaged, their reliability is also high. It is therefore important to consider the possibility that the chip has been deliberately damaged (for example, hit with a hammer) in order to circumvent the additional checks of the chip.

Merchants can help to minimize the rate of fallback transactions by keeping their terminals clean. Some manufacturers provide cleaning cards for dirty environments.
Good training is necessary to ensure that cashiers always insert the card correctly (cards inserted the wrong way round is one of the commonest reasons for failure) and that the card is always firmly pushed against the end stop. If the card fails to read first time, the usual recommendation is to try up to two more times before falling back to magnetic stripe.

If the magnetic stripe is read first, then the service code (2xx or 6xx) will indicate the presence of a chip, and the operator must be prompted to “dip” the card to read the chip. It must be possible (although it should not be too easy) for the operator to override this in the case of a genuinely faulty card; some terminals are able to test that a card has been physically inserted into the chip card slot and will not accept a fallback transaction if this has not happened. See, Technical appendix.

There are some marginal conditions in which it may be possible for the terminal to power up the chip, but not complete the transaction. There are rules that govern this situation – see the Technical appendix – however this will probably be a very unusual condition and most chip read failures are complete failures.

5.3 Authorization requirements

An authorization (online or by telephone, fax or telex) is required for any fallback transaction, regardless of the floor limit or transaction value; if this is not obtained then the transaction is at merchant risk.

5.4 Second level fallback

If, following the failure of a chip transaction, the magnetic stripe also cannot be read or the Longitudinal Redundancy Check (LRC) verification fails, a paper transaction may only be initiated for distress transactions. This must have been agreed with the acquirer, normally in cases where the cardholder has no other form of payment and the goods have already been dispensed or services performed. However, the transaction is at merchant risk unless an authorization by the issuer (or its agent) is obtained.

6. Acquirer perspective

All chip fallback transactions on a magnetic stripe have to be authorized by the issuer or its agent, even where the amount is below the relevant sector floor limit. Acquirers must be aware that both chip and fallback transactions may originate from cards issued by issuers in all parts of the world, some of which operate "no fallback" policies. To avoid chargebacks, the acquirers must send the fallback transaction online with the correct fields populated to the Issuer for approval/decline. This includes transactions with PIN.

Acquirers are recommended to acquirer transactions from terminals that have the capability to turn off fallback capability for domestic and international transactions at any time, preferable via a Terminal Management System (TMS).

6.1 Card Acceptance Devices

Acquirers must ensure that terminals are correctly set up to show a chip capability and, where appropriate, to indicate a fallback transaction in the Base I / SMS (Single Message System) message. IMPORTANT: If this is not done, the transaction is at acquirer risk, even where an authorization has been obtained.

The acquirer must populate the following fields to the issuer, indicating a fallback transaction:

- Field 60.2 (Terminal Entry Capability) = 5 (chip capable terminal), and
- Field 35 (Track 2) = 2xx or 6xx (indicating a chip card), and
- Field 22 Position 1-2 (POS Entry Mode) is not 05 and not 95[2]

(For additional information, see the Technical appendix)

6.2 Unattended acceptance terminals (UATs)

Depending on the type of UAT, a fallback may not be performed. An instance of this is when a chip is unreadable or if the transaction fails is declined and cannot be re-initiated using the magnetic stripe data. Regional or national requirements may allow/not allow technical fallback transactions at UATs.

6.2.1 ATMs

Chip-reading ATMs should offer fallback to magnetic stripe in the event that the chip reading fails. It is recommended that ATMs try a combination of cold resets and physical movement of the card (e.g. withdraw the card three millimeters; re-stage; reset; reset; reset; withdraw; re-stage; reset; reset; reset) before finally falling back to using the magnetic stripe data.

Despite this, the current experience is, that the rate of fallback at ATMs is somewhat higher than at POS, for reasons that are not completely understood today; typical figures are 1.5 – 3 percent. ATM owners should monitor rates of fallback transactions

[2] An acquirer in AP is liable for counterfeit loss when using POS Entry Mode Code 00 and 01.

and should investigate further any ATMs that show higher than three percent fallback rates or increasing levels of fallback.

Fallback beyond magnetic stripe is not allowed at ATMs.

6.2.2 UAT Type A

Since UAT Type A devices do not have the capability to send the transaction online for authorization, technical fallback must not be allowed. Type A UATs must verify the service code on the magnetic stripe and must not perform a magnetic stripe transaction if the service code indicates the presence of a chip.

6.2.3 UAT Type B and C

As with ATMs, UAT Type B and C have online capability, technical fallback may be allowed during the rollout period to provide good customer service as long as the reader is integrated i.e. the same reading device is reading both the chip and the magnetic stripe.

6.3 Second level fallback

Authorization by telephone, fax or telex is allowed as second fallback (if both chip to chip and magnetic stripe to magnetic stripe transactions fail). However it is very important that the issuer understands that the requested authorization is a fallback transaction or the transaction is at the acquirer's risk.

6.4 Blocked card / blocked application

If the chip on the card is blocked or the VSDC application in the chip is blocked, no fallback is allowed. The card acceptance device should be set up to decline the transaction if the card or the application is blocked. The logic in the terminal must not allow the next transaction to be a fallback transaction.

6.5 Declined transaction

When the card has decided that the transaction is declined, the terminal logic must not allow next transaction on the same card to be a fallback transaction on the same terminal.

6.6 Early Data Option

Early Data Option acquirers are required to respectively send and receive the new values in field 22 (POS Entry Mode) and field 60.2 (Terminal Capability), indicating if the authorization request originates from a fallback transaction.

6.7 Risk monitoring

Acquirers should monitor rates of fallback transactions on a terminal-by-terminal basis. High or rising rates of fallback may indicate a technical or maintenance problem with the terminal, insufficient staff training or merchant fraud.

6.8 Chargebacks

Acquirers should store BASE I transactions in case they need to prove which fields were populated in the authorization request to the issuer. An acquirer should also save any evidence of authorization requests via voice, fax or telex showing that information was given to issuer that the authorization request arise from a fallback transaction.

6.9 Referrals

Referrals are at the issuers risk provided that the acquirer has correctly indicated the transaction as fallback.

7. Issuer perspective

7.1 Card issuing

All Visa and Electron-branded chip cards must also carry a magnetic stripe and can therefore be used in magnetic stripe mode. The service code on the magnetic stripe (2xx or 6xx) indicates the existence of a chip.

Unlike most other aspects of card behavior, it is not in the issuer's control to determine whether fallback to magnetic stripe is allowed (since the assumption is that the chip data cannot be read). However, the issuer is able to determine the authorization response, and has the right to decline all fallback transactions.

7.2 Authorization systems and strategy

Although the full benefits of introducing chip will not be realized until fallback transactions are eliminated, most issuers will in practice allow fallback to magnetic stripe on most products, at least for a transition period, to avoid chip card customers feeling disadvantaged in relation to those with magnetic stripe cards. In order to permit this, an authorization strategy is required, and must be sufficiently flexible to allow a gradual removal of fallback and improvement in the risk profile.

Disallowing fallback from the start is a policy that could only be agreed at a national level (for competitive reasons) and would almost certainly be in response to a major counterfeit problem.

In order to implement an authorization strategy, issuers must first determine whether an authorization request is a fallback transaction. This involves checking the relevant fields in the Base I / SMS message that the acquirer must submit:

If the chip data fields are not present, but:

- Field 60.2 (Terminal Entry Capability) = 5 (chip capable terminal[3]), and
- Field 35 (Track 2) or 45 (Track 1) = 2xx or 6xx (indicating a chip card), and
- Field 22 Position 1 –2 (POS Entry Mode) is <u>not</u> 05 and <u>not</u> 95[4],

then this is a fallback transaction. Important: if these fields are not correctly populated by the acquirer, then the issuer will not be able to distinguish the transactions as fallback and liability will be the acquirers if fraud occurs. This includes transactions with PIN.

Any fallback transaction should increase the risk score of the transaction in relation to a chip transaction, however no technology is completely reliable and one of the benefits of using chip is that a fallback can be used if the chip card or reader fails. Most issuers will therefore want to accept fallback transactions, initially at least, but with more stringent criteria than for chip transactions or for magnetic stripe

[3] Including ATMs and UATs

[4] An acquirer in AP is liable for counterfeit loss when using POS Entry Mode Code 00 and 01. Other regions might present transactions with POS Entry Mode 00, 01 and 02.

transactions in magnetic-stripe-only terminals. Several other factors will be taken into account in determining the final risk score.

In addition, it is recommended that issuers maintain a number of counters, e.g. the number of fallback transactions in a month, the number of chip transactions since the last fallback transaction, the number of transactions since issued or last referral. Issuers with neural software should update these parameters and feed them to their neural system. Other issuers should develop some initial rules, e.g.:

- If this is a fallback transaction AND the number of chip transactions since the last fallback transaction < three AND number of transactions since issued or last referral > five, then investigate if re-issuance is necessary by contacting the cardholder
- If the number of fallback transactions this month / number of transactions this month > 0.5 AND number of transactions this month > 10, then schedule a re-issue

The effect of these rules should be monitored closely (e.g. once a month initially) and the values adjusted to give a suitable balance between close monitoring of fallback rates and fraud prevention.

Fallback transactions at ATMs should also be scored more highly for risk since there is no attending merchant who can check other security features on the card. However since the fallback to magnetic stripe at ATMs is relatively seamless, and there are no opportunities for collusive fraud, an increase in the risk score is probably the only appropriate response.

7.3 Further risk monitoring

In addition, periodic risk reports should track the rate of fraud and losses on fallback transactions and on chip transactions. This will allow issuers to determine the value of the initial risk score or weighting to be applied to fallback transactions. If the ratio exceeds a threshold, issuers should consider systematically declining all fallback transactions.

A more detailed strategy would involve looking for “hot spots” showing high rates of fraud on fallback transactions (typically overseas transactions) and adjusting the risk weighting upwards for these hot spots.

7.4 Second level fallback

Second level fallback transactions on chip cards (by telephone, fax or telex) increase the risk still further. Where High Coercivity (HiCo) magnetic stripes are used, the combined reliability of the chip and magnetic stripe is such that it is almost certain a second level fallback transaction means the card has been damaged or the terminal is not working. High preciousness should be made with second level fallback. However, an issuer can only make this decision if given the right information, i.e. that both chip and magnetic stripe technology have failed so it is essential that the acquirer pass the information to the issuer.

7.5 Early Data Option

Early Data Option issuers are required to respectively send and receive the new values in field 22 (POS Entry Mode) and field 60.2 (Terminal Capability), indicating if the authorization request originates from a fallback transaction.

7.6 Referrals

Referrals are at the issuers risk provided that the acquirer has correctly indicated the transaction as fallback.

7.7 Regional variances

Japan, Taiwan and Australia/New Zealand currently have more stringent rules than Visa. Other markets might introduce local rules regarding fallback