



:: dynamic currency conversion ::

FEXCO Centre :: Iveragh Road :: Killorglin :: Co. Kerry :: Ireland

Tel: +353 66 9761258 :: Fax: +353 66 9762242

[www.fexco.com](http://www.fexco.com)



## FALLBACK TRANSACTIONS ISSUER AUTHORISATION STRATEGY -

:: TABLE OF CONTENTS

:: 1. INTRODUCTION

:: 2. SUGGESTED STRATEGY

[ ] 2.1 Description

[ ] 2.2 Definition of terms

[ ] 2.3 Scenarios

:: 3. SUMMARY



:: dynamic currency conversion ::

FEXCO Centre :: Iveragh Road :: Killorglin :: Co. Kerry :: Ireland

Tel: +353 66 9761258 :: Fax: +353 66 9762242

[www.fexco.com](http://www.fexco.com)

## :: 1. INTRODUCTION

During the transition to use of PIN at Point of Sale, it is recommended that terminals should permit fallback to signature in the event that the PIN becomes locked or the cardholder is unable to remember the PIN. In these cases the transaction must be sent online to the issuer or its agent for authorisation.

It can be expected that some cardholders, on being allowed to use signature in fallback may deliberately lock their PINs, or take no action to seek a PIN re-advice or to unlock their PINs if the PIN becomes locked. This would allow them to continue to use signature until maturity, when fallback is switched off. Similarly, some cardholders may damage the chip in order to use magnetic stripe and signature. Unless controlled by issuers, such action will defeat the benefits of chip and PIN and also encourage fraudulent use.

It is, therefore, necessary for issuers to implement an authorisation strategy that helps cardholders who have genuinely forgotten their PINs, actively encourages them to request a re-advice of PIN and then unlock their cards, whilst managing potential fraud.

Whilst it is accepted that issuers will wish to implement their own authorisation strategies, this guideline is offered in order to ensure a common customer experience across a cardholder's cards, to maintain customer service and to promote an orderly and controlled migration to Chip and PIN by influencing cardholders' behaviour.

## :: 2. SUGGESTED STRATEGY

### :: 2.1 Description

The following suggested strategy should be considered by issuers in addition to any existing strategy. This strategy will allow cardholders to fall back to signature initially whilst they get used to using PIN at POS but will manage the future use of fallback to encourage full adoption and use of PIN at PoS.

There are five main categories of users that issuers should be able to identify through their authorisation systems:

- [ ] 1. Cardholder that has not used PIN before, or not used it with the currently used card.
- [ ] 2. Cardholder who regularly uses PIN successfully with card.
- [ ] 3. Cardholder who persistently locks their PIN, fails to unlock it, or tells the retailer that they have forgotten their PIN in the hope of PIN being bypassed.
- [ ] 4. Cardholder whose chip consistently fails – although this may be due to genuine chip failure.
- [ ] 5. The fraudster/thief attempting to use card without PIN.



:: dynamic currency conversion ::

FEXCO Centre :: Iveragh Road :: Killorglin :: Co. Kerry :: Ireland

Tel: +353 66 9761258 :: Fax: +353 66 9762242

[www.fexco.com](http://www.fexco.com)

## :: 2.2 Definition of terms

To identify these categories in their host systems, in addition to existing risk management functions, issuers will record the following data:

- [ ] **Successful PIN transactions** – Issuers should record in their authorisation systems information, from settlement data for each cardholder, the number of transactions that have been successfully performed using PIN. Such transactions can be identified from data in the Card Verification Results (CVR) – see section 3 below. Issuers should also include successful transactions performed with the card in ATMs, although these will not be identified from the CVR.
- [ ] **PIN unlock date** - Record the date when cardholder PIN unlock/change was most recently performed on this card.
- [ ] **PIN advice date** – Date when a PIN advice was most recently requested/generated for this card.
- [ ] **CVM fallback transactions** - Record the number of transactions where PIN Try Counter has been exceeded (PIN locked) or where the PIN was required and not entered (PIN bypass).  
**PIN User Threshold** - Allocate a threshold 'n' which represents the minimum number of successful PIN transactions for a cardholder to be considered to be accustomed to using PIN. This threshold may vary from issuer to issuer, and issuers may wish to use a different threshold for debit and credit products. As the rollout of chip and PIN progresses, issuers following this strategy are likely to reduce the PIN User Threshold gradually.
- [ ] **Re-advice period** – Period of 'grace' from issue of PIN re-advice to allow cardholder to receive advice and unlock PIN.
- [ ] **Technical fallback** – transactions where the chip cannot be read and which fall back to magnetic stripe. Issuers should record the total fallback transactions and also the total since last chip transaction.



:: dynamic currency conversion ::

FEXCO Centre :: Iveragh Road :: Killorglin :: Co. Kerry :: Ireland

Tel: +353 66 9761258 :: Fax: +353 66 9762242

[www.fexco.com](http://www.fexco.com)

### :: 2.3 Scenarios

**Scenario 1** - If a cardholder has successfully performed 'n' or more chip and PIN transactions (exceeded PIN User Threshold) and the next authorisation request indicates CVM fallback, the issuer may assume that the cardholder is conversant with use of PIN and that this may be a fraudulent transaction. The authorisation may then be declined.

**Scenario 2** – If a cardholder has not used PIN with their chip and PIN card, or has used it less than 'n' times with PIN (PIN transactions less than PIN threshold), the issuer may allow fallback to signature for a period. This period may be determined by the number of CVM fallback transactions or by the re-advice period. The issuer should take into account whether the cardholder has contacted the issuer to seek a re-advice of PIN. This should enable cardholders who do not want to use PIN to be controlled.

**Scenario 3** – Cardholder has not performed PIN transactions or has performed less than the PIN threshold and transactions in Technical fallback are received. The chip may be genuinely damaged or the cardholder may have damaged it. Issuers should monitor the number of Technical fallback transactions and, if appropriate, contact the cardholder to identify if there is a problem with the card and, if necessary, issue a replacement.

Issuers should ensure that a clear message is given to cardholders that whilst they may be offered the use of signature if they have forgotten their PIN or if their PIN is locked, they should not rely upon the transaction being accepted by the issuer.



:: dynamic currency conversion ::

FEXCO Centre :: Iveragh Road :: Killorglin :: Co. Kerry :: Ireland

Tel: +353 66 9761258 :: Fax: +353 66 9762242

[www.fexco.com](http://www.fexco.com)

### :: 3. SUMMARY

The primary need in the strategy is to identify those cardholders that are genuinely having difficulty with their PIN. These are expected to be people that have not used PIN successfully with their card. Once actions have been taken to help these cardholders, their PIN use needs to be monitored to ensure that they have taken action to unlock their PINs and are then continuing to use PIN.

Secondly, issuers need to identify cardholders who have been successfully using PIN with their cards and then appear to have locked or forgotten their PIN. These could be considered to be suspect transactions that may need special action.

Thirdly, issuers need to identify cardholders that are persistently locking their cards so that they may be encouraged to start using PIN. If necessary the issuer will start to decline fallback, PIN locked and PIN bypass transactions.

Some issuers may wish to take a strong line in managing signature fallback by setting a PIN Threshold of '1' from the start. However, experience from the introduction of PIN in Japan where fallback to signature was not allowed, led to significant customer service issues. It is considered that setting a threshold of between 3 and 5 and reducing it over time to 1 should provide a balance between customer service and fraud management.