Visa system integrity programme update

Introduction

The purpose of this document is to advise you of new Visa rules that will commence from April 2021 on authorisation decline reason codes.

What is changing?

Starting in April 2021, Visa will introduce new rules which when implemented will:

- Cluster existing decline response codes into four categories and require Issuers to use descriptive values when they are unable to approve a transaction
- Limit authorisation reattempts to a maximum of 15 over 30 days
- Data Quality – Category 3 declines exceed 25,000 attempts in a 30-day rolling period in Europe

In October 2021 Visa increases the rule to:

- Prohibit reattempts against certain response codes (Category 1)

In addition, on a date as yet to be agreed, but by way of advance notice:

- Require consistent use of key data elements in Merchant reattempts

Decline Code Categories

Category 1: Issuer will never approve (Reattempt Not Allowed) - Decline response codes that indicate the account never existed or has been permanently blocked including lost or stolen account numbers. This category also includes decline codes that indicate the account is valid however the transaction is not permitted due to permanent product/regulatory restrictions or transaction error conditions that prevent approval. A Merchant or Acquirer should not reattempt authorisation.

Category 2: Issuer cannot approve at this time (Reattempt Allowed)
Decline response codes that indicate the Issuer may approve, but cannot do so now, perhaps due to temporary decline condition such as credit risk, Issuer velocity controls or other account restrictions. This cluster covers temporary decline decisions made by Issuers that may change over time and the Issuer would welcome a future authorisation attempt. In some cases, cardholder action is required to remove the restriction before an approval can be obtained.

Category 3: Data quality (Revalidate data prior to reattempt)
Decline codes that indicate data quality issues where invalid payment or authentication data has been provided and the Issuer may approve if valid information is provided. High occurrences of response codes in these categories may indicate insufficient Merchant risk protection controls such as velocity checks and pre-validation of basic account information (e.g. Mod-10 or expiry date).

Category 4: Generic response codes (Reattempt allowed)
The majority of decline response codes fall into the above categories; however generic response codes may be used on an ad-hoc basis when a decline condition does not correspond to a descriptive value. This category includes all other decline response codes, many of which provide little to no value to Acquirers/Merchants in determining their reattempt strategy and their usage should remain minimal.

What does this mean for me?

Outlined in the tables below are the actions that you will need to implement to ensure compliance with the new Visa rules.

Decline code categories and expected behavior and rules

Decline Category	Action needed	Criteria
1	Merchants must not reattempt the transaction and should exclude the transaction from automated retry processing.	Any reattempt on a category 1 transaction at the MID level within a rolling 30 day period.
2,3 & 4 (Footnote 1)	Limit reattempts to 15 in a rolling 30 days	Same transaction at the MID level within a rolling 30-day period
3	Ensure legitimate purchase data has been provided (e.g.-mod-10, exp. date, etc.) and display messaging on POS terminal or payment page to prompt the customer/cashier to correct invalid payment information	Separate from the 15 over 30, Visa will be monitoring category 3 declines and it is expected to not have more than 25K cat 3 declines on a MID within a rolling 30 days.
All Categories	Merchants must not manipulate data elements that identify the Merchant type, location or transaction environment in reattempted transactions	Do not manipulate the data elements below in a reattempt: •*Acquirer or Merchant Country* •*Merchant Category Code (MCC)* •*POS Condition Code* •*POS Environment Field* •*POS Entry Mode* •*Electronic Commerce Indicator (ECI) codes* **Implementation date is TBD**

1 – Until October 2021 Category 1 falls within the same 15 reattempts within a rolling 30 days.

Starting in April 2021 Elavon will start transitioning to a more descriptive decline response reason code, please refer to the table below. This will allow you to determine which Visa category the decline falls into. Please ensure that you amend your procedures and potentially systems to reflect the new Visa rules and to prevent reattempting declines that may break the rules.

Category	Reason Code	Description	reply_code	reply_1_text	
1	3	Invalid Merchant	5279	INVALID MER ID	
1	4	Pick Up Card (no fraud)	7004	PICK UP CARD SPC	
1	7	Pick Up Card - special	7007	PICK UP CARD SPC	
1	12	Invalid Txn	7012	INVALID TX	
1	15	No such issuer	7015	NO SUCH ISSUER	
1	41	Lost card - pick up	7041	LOST PICKUP CARD	
1	43	Stolen card - pick up	7043	STOLEN CARD	
1	46	Closed Account	7046	CLOSED ACCOUNT	
1	57	Txn not permitted to C/H	7057	TX NOT PERMITTED	
1	62	Restricted Card	7062	RESTRICTED CARD	
1	93	Txn cannot complete - law	7093	TX CANT COMPLETE	
1	R0	Stop payment order	7130	STOP PAYMENT ORD	
1	R1	Revoc of auth order	7131	REVOC AUTH ORDER	
1	R3	Revoc of all auth orders	7133	REVOC ALL AUTH	
2	19	Re-enter txn	5270	PLEASE RETRY5270	
2	51	Insufficient Funds	7051	INSUFF FUNDS	
2	59	Suspected Fraud	7059	SUSPECTED FRAUD	
2	61	Exceeds Approval Amt Lmt	7061	EX APPROVAL AMT	
2	65	Exceeds Withdrawal Freq Lmt	7065	EX W/DRAWL FREQ	
2	75	PIN Retries exceeded	5571	PIN TRIES EXCEED	
2	78	Blocked First Used	7078	BLOCKED 1st USE	
2	86	Cannot Verify PIN	7086	CANT VERIFY PIN	
2	91	Issuer Unavilable	7091	ISS/SW INACTIVE	
2	96	System malfunction	7096	SYS MALFUNCTION	
2	N3	Cash Service Not Avail	5736	CASH SRV UNAVAIL	
2	N4	Cash Serv exceeds apprv lmt	5737	CASH REQ EXCEED	
3	14	Invalid account number	5271	INVALID CARD	
3	54	Exp Card or missing exp date	5306	EXPIRED CARD	
3	55	Incorrect PIN	5218	INCORRECT PIN	
3	82	Neg online CVV results	7082	NEG ONLINE DATA	
3	N7	Incorrect CVV	7107	INCORRECT CVV	
3	IA	Addtl cust authent reqd	5371	INSERT CARD	
3	70	PIN Data Reqd	5222	DECLINED	

Elavon Financial Services DAC. Registered in Ireland – Number 418442. Registered Office: Building 8, Cherrywood Business Park, Loughlinstown, Co. Dublin, D18 W319, Ireland.
Elavon Financial Services DAC, trading as Elavon Merchant Services, is regulated by the Central Bank of Ireland.

Elavon Financial Services DAC. Registered in Ireland with Companies Registration Office. The liability of the member is limited. United Kingdom branch registered in England and Wales under the number BR022122.
Elavon Financial Services DAC, trading as Elavon Merchant Services, is authorised and regulated by The Central Bank of Ireland. Authorised by the Prudential Regulation Authority and with deemed variation of permission. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details of the Temporary Permissions Regime, which allows EEA-based firms to operate in the UK for a limited period while seeking full authorisation, are available on the Financial Conduct Authority's website.

03/2021