

New Rules and Fees to Enhance Ecosystem Risk Performance

LAC | Acquirers, Issuers, Processors

Visa, Interlink, Plus Networks



Overview: Visa is introducing a set of new rules and fees to ensure clients properly use declined transaction response codes that will serve to improve authorization and mitigate invalid transactions.

Visa's vision is to be the best way to pay and be paid by everyone, everywhere. To achieve this, our mission includes being the most trusted and secure digital payment network that enables individuals, businesses and economies to thrive. To that end, Visa is seeking to drive positive payments ecosystem behavior through commercial fees, rather than just traditional compliance programs, providing clients with more direction and requirements over their use of declined transaction response codes.

Visa will introduce new decline code rules **effective 18 April 2020**, with related fees **effective 1 April 2021**, to ensure that all participants properly use transaction decline codes and ensure authorization consistency. Fees will apply where clients are non-compliant with the Visa Rules, as defined within this article.

Enhancing Decline Code Management

Authorization processing requires a careful balance among participants. Ensuring appropriate information flow is critical to creating optimal behavior.

An extensive review of the authorization approach highlighted that decline codes currently provide limited value, as many issuers default to selecting a single code for all declines or use definitions that provide minimal value to acquirers and merchants. This practice is creating a high volume of poorly focused merchant retry attempts, since merchants cannot easily tell a low-risk decline (e.g., lack of funds or small processing glitch) from a high-risk one (e.g., blocked card or incorrect data submitted), which results in increased costs, damaged detection processes and confused consumers.

Visa will reposition decline response codes to make them more useful while minimizing cost-creating or damaging behaviors. The existing decline codes will be grouped into categories that issuers will be expected to operate across when handling authorization requests, which will require changes to response code processing.

In consultation with clients and merchants, Visa will cluster the decline codes already in the system into the four categories below:

- **Category 1—Issuer will never approve:** A sub-set of decline codes that indicates the card is blocked for use or never existed and means there is no circumstance in which the issuer will grant an approval—for example, in the case of a lost or stolen card. Any attempt to authorize a transaction that has previously received a

Category 1 decline will incur a fee. An issuer approval after an initial Category 1 decline response will be subject to non-compliance enforcement actions.

- **Category 2—Issuer cannot approve at this time:** A sub-set of decline codes that indicates the issuer may approve but cannot do so now, perhaps due to a system issue or a lack of funds. This cluster covers temporary decline decisions made by issuers that may change over time. It occurs when the issuer is prepared to approve a transaction, but is unable to do so at the time and would welcome a further authorization attempt in the future—for example, as in the case of insufficient funds decline code.

Visa will apply a transaction fee for the 16th and subsequent reattempted transactions.

- **Category 3—Issuer cannot approve with these details:** A sub-set of decline codes that indicates the issuer cannot approve based on the details provided, such as an invalid account number, incorrect Card Verification Value (CVV) or CVV2, or incorrect expiration date.

With the continued growth of e-commerce business, Visa is increasingly seeing fraudsters performing enumeration attacks (also known as brute force / testing attacks) in an attempt to determine valid card, expiration and CVV2 data. These attacks are typically mitigated by merchants, but many do not have effective controls, which leads to increased costs and generates issuer complaints for invalid transactions. As such, Visa will deploy a framework that applies per-transaction fees to acquirers that do not control these types of invalid transactions.

The fee will operate at the merchant level, but will be zero for the first 10,000 declines in a 30-day period to account for some degree of typical mis-keying of payment data.

- **Category 4—Generic response codes:** While the great majority of declines fall into the above categories, issuers may use some special codes on an ad-hoc basis. However, their usage should remain minimal. This category includes all other decline codes, many of which are of a technical nature or provide little to no value to acquirers and merchants. Visa will expect issuers to use appropriate and balanced response codes between the three previous categories, limiting the use of Category 4 to no more than 5% of their total declines. Issuers that only respond to authorization requests with a Category 4 decline (generic response codes) or exceed the 5% limit will incur a fee.

With the introduction of the new generic response codes fee, Visa will remove the existing Negative Response Fee and provide timelines for the removal in a future communication.

Declined Transaction Resubmission

The Visa Rules allow a maximum of four authorization re-attempts over a 16-day period, but in practice, merchants will process attempts far in excess of this limit, creating increased costs and lower approval rates. To redress this, and drive an uplift in approval rates, Visa will modify this rule to allow up to 15 reattempts in a 30-day period for Categories 2, 3 and 4 declines. Visa will apply a transaction fee for the 16th and subsequent reattempted transactions.

To support the adoption of this streamlined categorization, the Visa Rules regarding the use of response codes will be modified **effective 18 April 2020**. Visa will assess the following fees associated with the above criteria to LAC clients on a per-transaction basis **effective 1 April 2021**.

Perspective	High-Risk Transaction Criteria	Domestic Fee ¹	Cross-Border Fee
Acquirer	Category 1: Issuer will never approve Fee applies on reattempt after initial decline.	USD 0.10	USD 0.25
Acquirer	Category 2: Issuer cannot approve at this time Fee applies for the 16th and subsequent reattempts.	USD 0.10	USD 0.25
Acquirer	Category 3: Issuer cannot approve with these details Fee applies for the 16th and subsequent reattempts, and/or subsequent transactions exceeding 10,000 / month per merchant.	USD 0.10	USD 0.25
Issuer	Category 4: Generic response codes Fee applies for Category 4 declines exceeding 5% of total declines.	USD 0.10	USD 0.25
Acquirer	Category 4: Generic response codes Fee applies for the 16th and subsequent reattempts.	USD 0.10	USD 0.25

¹ Domestic transactions are defined as where the issuer and the merchant are in the same country.

Ensuring Authorization Consistency

It has become common practice among some merchants and acquirers to amend various data fields following an issuer decline to seek a gap in issuer authorization controls and detection systems in order to achieve an approval. This data manipulation is damaging to the Visa system as well as the issuer's ability to authorize transactions effectively and consistently. To that end, Visa will introduce fees to ensure data consistency.

Data Consistency

Visa will apply an acquirer-based fee to enforce merchant and acquirer data field consistency. Visa will not permit acquirers to change or manipulate data elements in an authorization reattempt, aside from the transaction amount. These elements will include but not be limited to merchant country, merchant category code, POS condition code, POS environment field, POS entry mode and electronic commerce indicator. The fee will apply when a merchant / acquirer resubmits an authorization with changed data elements following a decline.

The following fees associated with the above criteria will be **effective 1 April 2021**.

Perspective	High-Risk Transaction Criteria	Domestic Fee ¹	Cross-Border Fee
Acquirer	Data consistency	USD 0.10	USD 0.25

¹ Domestic transactions are defined as where the issuer and the merchant are in the same country.

Decline Response Codes by Category

An issuer must attempt to approve or partially approve an authorization request for any valid account number in good standing. If an issuer is unable to approve a transaction, it must use a decline response code that most accurately reflects the reason for the decline.

To ensure acquirers and merchants are able to identify the reason for a declined transaction, a VisaNet processor must not alter an issuer's decline response code. Processors must be capable of supporting an issuer's decline response mapping according to the categories below.

Category 1 (Issuer will never approve)	Category 2 (Issuer cannot approve at this time)	Category 3 (Issuer cannot approve with these details / Data quality issues)
<ul style="list-style-type: none"> 03 (Invalid merchant) 04 (Pickup card) 07 (Pickup card, special conditions) 12 (Invalid transaction) 15 (No such issuer) 41 (Pickup card [lost card]) 43 (Pickup card [stolen card]) 57 (Transaction not permitted to cardholder) 62 (Restricted card) 78 (No account) 93 (Transaction cannot be completed) R0 (Stop payment order) R1 (Revocation of authorization order) R3 (Revocation of all authorization) 	<ul style="list-style-type: none"> 19 (Re-enter transaction) 51 (Insufficient funds) 59 (Suspected fraud) 61 (Exceeds withdrawal amount limits) 65 (Exceeds withdrawal frequency) 75 (Allowable number of PIN-entry tries exceeded) 86 (ATM malfunction) 91 (Issuer or switch is inoperative) 96 (System malfunction) N3 (Cash service not available) N4 (Cash request exceeds issuer limit) 	<ul style="list-style-type: none"> 14 (Invalid account number) 54 (Expired card) 55 (Incorrect PIN) 82 (Negative Online CAM,² dCVV,³ iCVV⁴ or CVV results) N7 (Decline for CVV2 failure [Visa])

² Cardholder Authentication Method

³ Dynamic CVV

⁴ Integrated Chip Card CVV


Additional Resources

[Enhance Ecosystem Risk Performance \(Advance Copy\)](#)

Note: For Visa Online resources, you will be prompted to log in.

For More Information

Contact your Visa representative. Merchants should contact their acquirer.

Notice: This Visa communication is furnished to you solely in your capacity as a customer of Visa Inc. (through its operating companies of Visa U.S.A Inc., Visa International Service Association, Visa Worldwide Pte. Ltd, Visa Europe Ltd., Visa International Servicios de Pago España, S.R.L.U. and Visa Canada Corporation) or its authorized agent, or as a participant in the Visa payments system. By accepting this Visa communication, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in the Visa Rules, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or as a participant in the Visa payments system. You may disseminate this Information to a merchant participating in the Visa payments system if: (i) you serve the role of "acquirer" within the Visa payments system; (ii) you have a direct relationship with such merchant which includes an obligation to keep Information confidential; and (iii) the Information is designated as "affects merchants" demonstrated by display of the storefront icon  on the communication. A merchant receiving such Information must maintain the confidentiality of such Information and disseminate and use it on a "need to know" basis and only in their capacity as a participant in the Visa payments system. Except as otherwise provided, the Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Visa is not responsible for errors in or omissions from this publication.