Visa Business News

E-commerce & Authentication

20 May 2021

Avoid Authorization Declines by Following the Requirements for Token Cryptograms

Global | *Acquirers, Processors, Agents*

Visa, Interlink, Plus Networks; V PAY; Europe Processing

Overview: Token cryptograms must be new and unique for each authorization request, and must not be stored beyond the authorization request. Effective 30 January 2022, a resubmitted or stale token authentication verification value or dynamic token verification value will result in a declined authorization request.

Effective since the April 2016 Business Enhancements release, acquirers have been required to ensure merchants can send authentication data in token-based card-on-file (COF) and e-commerce transactions, including in-app e-commerce. Token authentication verification value (TAVV) and dynamic token verification value (DTVV) cryptograms are generated by an approved entity, such as Visa Token Service, then passed to the merchant via the token requestor. The merchant must then submit an unchanged TAVV or DTVV in the authorization request.

Mark Your Calendar:

- Transactions including a previously used or stale TAVV or DTVV will be declined **(30 January 2022)**

The Visa Rules require that agents and merchants must not store TAVV or DTVV cryptograms (in addition to Card Verification Value 2 and Cardholder Authentication Verification Value) subsequent to authorization (ID#: 0002228).

With the October 2019 Business Enhancements release, Visa reminded acquirers and their merchants to comply with the above rules and requirements to avoid transaction declines.

Enforcement of Rules for Token Cryptograms

Effective 30 January 2022, Visa will decline any transaction including a previously used or stale TAVV or DTVV. This is essential to ensure the integrity of cryptograms as a key token domain control and prevent fraud.

To avoid declined authorization requests, acquirers and their merchants must ensure they comply with the following existing rules and requirements regarding TAVV and DTVV cryptograms for cardholder-initiated, token-based COF and e-commerce transactions, including in-app e-commerce:

- The TAVV and DTVV cryptograms must be new and unique for each authorization request.
- The TAVV and DTVV cryptograms are one-time use.
- The TAVV and DTVV must not be stored beyond the authorization request.

- The TAVV, DTVV and electronic commerce indicator values provided by the token requestor must be unchanged when submitted in the authorization request message.
- **A resubmitted or stale TAVV or DTVV will result in a declined authorization request.**
- Merchant-initiated transactions must follow the merchant-initiated transaction framework, and do not include token cryptograms.

For More Information

Merchants and third party agents should contact their acquirer.

© Visa. All Rights Reserved.