Acceptance   20 August 2020

In-App Transaction Identification Reminders

Global | *Acquirers, Issuers, Processors, Agents*
Visa Network

Overview: Application-based mobile payment transactions are quickly expanding into additional merchant segments. To limit unnecessary declines, Visa encourages clients to be aware of this transaction method.

Application-based (also known as in-app) mobile payment transactions, where cardholders use their mobile devices to make purchases on merchant applications, continue to expand to additional merchant segments. In particular, this credential-not-present transaction type is moving into segments that traditionally contained only credential-present transactions.

Visa reminds acquirers and processors with merchants conducting in-app payments to submit authorizations with the correct credential-not-present transaction identifiers and follow the stored credential rules and requirements.

Issuers should be aware that legitimate credential-not-present transactions may now occur in some merchant segments that have historically been credential-present.

Merchant Transaction Elements

To ensure consistency across the Visa system, merchants and acquirers submitting authorizations for in-app transactions should correctly code them as indicated below:

Authorization Fields	Change From Credential-Present Transaction Values?	In-App Transaction Values
Field 18 (Merchant Category Code)	No	As appropriate for merchant
Field 22 (POS Entry Mode)	**Yes**	01 (Manual Key Entry)[1] or 10 (credential-on-file [COF])
Field 25 (POS Condition Code)	**Yes**	59 (e-commerce)
Field 60.8 (Electronic Commerce Indicator)	**Yes**	Varies by authentication type
Field 126.13 (POS Environment)	**Yes**	C (COF)[2] or not present[3]

[1] A POS entry mode of 01 (Manual Key Entry) is used when credentials are not being stored or when the consumer is making their purchase and is requesting at the time to store credentials for future use.

[2] The value "C" in the POS Environment field with a POS entry mode of 01 indicates the consumer is requesting to store credentials for future use at the time of purchase.

[3] No POS Environment field with a POS entry mode code of 10 indicates cardholder-initiated, stored credential transactions.

Stored Credential Framework Requirements

Acquirers and merchants must ensure that in-app payments comply with Visa's rules and requirements for stored credential transactions. These include:

- Obtaining cardholder consent for initial storage of credentials

- Utilizing appropriate data values (i.e., stored credential indicators as per the Stored Credential Transaction Framework) to identify initial storage and usage of stored payment credentials

- Submitting an account verification authorization if no amount is due at the time credentials are stored

More details on stored credential rules and requirements can be found in *Improving Authorization Management for Transactions with Stored Credentials* (not available to merchants).

Issuer Transaction Processing

With the increase of in-app payments, issuers should ensure that their authorization systems are not set to automatically decline authorizations solely because they are identified as credential-not-present from some merchant segments that have traditionally submitted credential-present transactions.

For More Information

Merchants and third party agents should contact their acquirer.

Article ID: AI10262