Visa Business News

E-Commerce & Authentication

31 August 2023

Visa Secure Program Updates: 12 Data Fields Required for EMV 3-D Secure Minimum Data Requirements and Amendments to Visa Secure Disputes

Global | *Acquirers, Issuers, Processors, Agents*

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

Overview: The *Visa Secure Program Guide*, a supplemental guide to the Visa Rules, will be updated to include 12 required data fields in the authentication request message for data quality monitoring. These existing data fields were previously categorized as "required conditional." In addition, amendments have been made to only assess authorization data to determine fraud dispute rights.

To support the payments ecosystem in realizing the full benefits of Visa Secure EMV® 3-D Secure (3DS) authentication, the *Visa Secure Program Guide*, a Visa Supplemental Requirements document, has been updated with the following changes:

Mark Your Calendar:

- Merchants must provide 12 data fields for EMV 3DS AReq messages **(12 February 2024)**

- Twelve data elements have been recategorized from "required conditional" to "required" in the *Visa Secure Program Guide*. This change will be **effective 12 February 2024**.
- The *Visa Secure Program Guide* will be amended to only require authorization for Visa Secure Visa Resolve Online logic **effective 15 April 2024**.

Twelve Additional Data Fields Required for EMV 3DS Authentication Requests

Merchants must provide complete and accurate transaction data in their authentication requests. Merchants must also ensure that the 3DS Method URL completes the collection of device data to support successful authentication if the 3DS Method URL is provided by the issuer.

When using Visa Secure, high-quantity and high-quality data will provide benefits across the entire ecosystem.

Based on the upcoming changes to the *Visa Secure Program Guide*, for EMV 3DS minimum data requirements, **effective 12 February 2024**, merchants must provide the following data fields in their authentication request (AReq) messages. The following data fields have been updated from "required conditional" to "required." The guide will be updated once the changes are implemented.

- Browser IP Address[1]
- Browser Screen Height[1]
- Browser Screen Width[1]
- Cardholder Billing Address City[2]

- Cardholder Billing Address Country[2]
- Cardholder Billing Address Line 1[2]
- Cardholder Billing Address Postal Code[2]
- Cardholder Billing Address State[2]
- Cardholder Email Address
- Cardholder Name
- Cardholder Phone Number (Work / Home / Mobile) (At least one of these fields must be provided)
- Common Device Identification Parameters (Device IP Address)[3]

For more information on the Visa Secure minimum data requirements for EMV 3DS, refer to the *Visa Secure Program Guide* on the Visa Secure Documentation page at Visa Online.

As a reminder, the *Visa Secure Program Guide* defines some fields as "required conditional." The merchant must include these data fields in their AReq if the conditional inclusion requirements are met. For example, shipping address data fields must be provided for transactions that require delivery.

Note: The minimum data requirements do not apply if there are local data privacy regulations that prohibit the data field from being shared.

[1] Only for browser-based transactions

[2] Except in countries where the billing address fields do not exist

[3] Only for Software Development Kit (SDK) transactions

Consistent and High-Quality Data Helps Enhance Business Outcomes for Merchants, Cardholders and Issuers

When merchants leverage authentication through Visa Secure, issuers are trusted to detect fraudulent transactions. Key data elements in every AReq message are critical to supporting an issuer in making accurate risk assessments for successful authentications.

When merchants provide these 12 priority data fields in their AReq messages, the following benefits can be achieved across the entire EMV 3DS ecosystem globally:

- Merchants see an authentication success rate lift of +4% and an approval rate lift of +6%.[4,5]
- Issuers can see a +65% fraud detection rate (FDR) lift.[6]

Visa Secure is designed to provide a frictionless experience for Visa cardholders. Enhanced data quality may deliver more seamless experiences, increased security confidence and fewer false declines to cardholders.

- Cardholders receive a better experience through a +57% frictionless rate lift.[5]

[4] The dataset for these calculations contains 95% of Visa Secure global transactions that occurred during the months of February–March 2022. The uplift figures were generated by merchants based on the rate at which they populate the priority data elements and averaging their product performance. For more information, please refer to the global business cases in *the Global—Better Data Best Practices Guide for Visa Secure*, available in the Merchant Resources section of the Visa Secure Services Library.

[5] Based on merchants that populate more than 50% of the priority data elements.

[6] The dataset for this analysis contains Visa global transactions that were reported as fraud during the month of August 2021. The FDR performance uplift was calculated by comparing the performance of a Visa fraud detection model in the scenario when priority data elements were present versus when they were replaced by null or default values used in the risk-based authentication (RBA) model.

Issuer Best Practices to Leverage Data Quality

Issuers must use RBA to analyze transactional data provided by the merchant. In cases where the merchant provides all the mandatory data fields, issuers should consider the level of risk associated with that transaction. In low-risk scenarios, issuers should authenticate frictionlessly to provide the cardholder with a better experience. When making authentication decisions, issuers should utilize the following strategy for transactions:

- Truly low-risk transactions are seamlessly authenticated.
- Moderate or medium-risk transactions are challenged.
- High-risk transactions are declined.

The Visa Analytics Platform offers the 3DS Authentication Report, which allows subscribed issuers to view their authentication performance. Issuers can analyze authentication success rate, challenge / frictionless rates and the abandonment rate, and can leverage these insights and work with their access control server (ACS) providers to update their authentication strategy to optimize performance.

Issuers must remain in compliance with the Visa Secure Performance Program to ensure a positive e-commerce experience for cardholders. As a reminder, issuers must not exceed a cardholder abandonment rate of 5% for EMV 3DS transactions. Evaluating the risk level of each transaction using RBA to make authentication decisions can lead to a lower cardholder abandonment rate. For more information on the Visa Secure Performance Program requirements, refer to the *Visa Secure Program Guide* on the Visa Secure Documentation page at Visa Online.

Visa Secure Disputes Update

Currently, outside of the U.S. region, Visa Secure fraud dispute rights are determined based on both authorization and clearing data. To streamline the Visa Secure dispute process and align with all other Visa dispute processes, **effective 15 April 2024**, all fraud dispute rights for Visa Secure will be determined based on authorization data only.

As part of the Visa Secure program, merchants / acquirers are required to submit the same electronic commerce indicator (ECI) value in clearing that was submitted in authorization for both ECI 05 and ECI 06 transactions. Visa recommends that issuers and acquirers monitor authorization and clearing records to ensure that transactions are processed with the correct ECI values.

Additional Resources

Documents & Publications

"Launch of Issuer 3DS Authentication Dashboard in Visa Analytics Platform," *Visa Business News,* 27 July 2023

Online Resources

Refer to the following documents on the Visa Secure Documentation page at Visa Online for additional information:

- *Visa Secure Program Guide*

- *Visa Secure Using EMV 3DS Best Practices for Merchants*
- *Minimum Data Requirements for Merchants*
- *Visa Secure Using EMV 3DS Best Practices for Issuers*
- *RBA Best Practices: Improving Risk Based Authentication with Visa Secure with EMV® 3-D Secure*
- *Visa Secure Dispute Resolution Guide*

Refer to the merchant data quality global and regional business cases in the Better Data Best Practices guides for Visa Secure in the Merchant Resources section of the Visa Secure Services Library.

Visa Analytics Platform

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

For More Information

AP, CEMEA: Contact your Visa representative.

Canada and U.S.: Contact eSupport@visa.com.

Europe: Contact Visa customer support on your country-specific number, or email CustomerSupport@visa.com.

LAC: Create a case in the Visa Support Hub.

Merchants and third party agents: Contact your acquirer, issuer, processor or Visa representative.

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