Visa Business News

E-Commerce & Authentication

4 January 2024

Updates to Visa Secure Data Field Mandate: Required Data Fields Reduced and Effective Date Extended

AP, Canada, Europe, LAC, U.S. | *Acquirers, Issuers, Processors, Agents*

Visa, Plus Networks; V PAY; Europe Processing

Overview: Visa is announcing changes to the Visa Secure data field mandate originally communicated in the 31 August 2023 edition of the *Visa Business News*. The effective date has been updated to 12 August 2024 and the number of required data fields has been reduced.

In AI13277 in the 31 August 2023 edition of the *Visa Business News*, Visa announced changes to the *Visa Secure Program Guide*, a Visa Supplemental Requirements document, to include 12 additional required data fields which would be effective 12 February 2024.

Mark Your Calendar:

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

Based on ecosystem feedback and further analysis, Visa will reduce the 12 required data fields to five required data fields for browser transactions or three required data fields for in-app transactions. Additionally, to provide the ecosystem with more time to prepare for the new requirements, Visa is updating the effective date to **12 August 2024**.

The newly required data fields only apply to standard Visa Secure EMV® 3-D Secure (3DS) payment transactions (PAs). Non-payment transactions (NPAs) and 3DS requestor-initiated (3RI) transactions will not require these additional data fields as part of the mandate. Additionally, this Visa Secure data field mandate does not apply to Digital Authentication Framework (DAF) transactions.

Updated Minimum Data Requirements for EMV 3DS Authentication Requests

Effective 12 August 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 *Visa Secure Program Guide* will be updated effective 12 August 2024 to reflect these minimum data requirement changes.[1]

Note: Per the *Visa Secure Program Guide* and the Visa Rules (ID#: 0000385), the minimum data requirements do not apply if there are local data privacy regulations that prohibit the particular data field from being shared.

As a reminder, merchants must provide complete and accurate transaction data in their authentication requests.

Data Field Requirements by Device Channel

Browser	In-App / Software Development Kit (SDK)
Browser IP Address	Common Device Identification Parameters (Device IP Address)
Browser Screen Height	
Browser Screen Width	
Cardholder Phone Number[2] OR Cardholder Email Address[3]	Cardholder Phone Number[2] OR Cardholder Email Address[3]
Cardholder Name	Cardholder Name

Consistent high quantity and high quality of data fields help enhance business outcomes for merchants, cardholders and issuers. Despite the update in minimum requirements outlined above, Visa continues to recommend that merchants provide all 12 of the following priority data fields,[1] as more data supports issuers' authentication decision-making.

Priority Data Fields	Requirement Status	Update From AI13277 Announcement
Browser IP Address[4]	Mandatory (Browser)	No Update
Browser Screen Height[4]	Mandatory (Browser)	No Update
Browser Screen Width[4]	Mandatory (Browser)	No Update
Cardholder Billing Address City[5]	Recommended[1]	No Longer Mandatory
Cardholder Billing Address Country[5]	Recommended[1]	No Longer Mandatory
Cardholder Billing Address Line 1[5]	Recommended[1]	No Longer Mandatory
Cardholder Billing Address Postal Code[5]	Recommended[1]	No Longer Mandatory
Cardholder Billing Address State[5]	Recommended[1]	No Longer Mandatory
Cardholder Email Address[3]	Mandatory (Browser / In-App)	Mandatory (unless Cardholder Phone Number is provided)
Cardholder Name	Mandatory (Browser / In-App)	No Update
Cardholder Phone Number (Work / Home / Mobile)[2]	Mandatory (Browser / In-App)	Mandatory (unless Cardholder Email is provided)
Common Device Identification Parameters (Device IP Address)[6]	Mandatory (In-App)	No Update

[1] The remaining seven fields of the 12 originally communicated as being required in AI13277 will be reverted to "required conditional" with the next publication of the *Visa Secure Program Guide*.

[2] At least one phone number out of work, home or mobile must be provided.

[3] It is recommended to provide both phone and email data fields for authentication; however, if the merchant only collects one of the data fields, then providing one of the two options satisfies the minimum data requirement.

[4] Only for browser-based transactions

[5] Except in markets where the billing address fields do not exist

[6] Only for SDK transactions

Frequently Asked Questions

What is the purpose of providing these additional data fields for EMV 3DS?

- EMV 3DS is a data-driven solution that relies on true cardholder data for issuers to make accurate authentication decisions. For information on how additional data in the EMV 3DS AReq benefits merchants,

cardholders and issuers, please reference the business cases available on the Visa Secure Services site (under the Visa Secure Services [VSS] Library "Merchant Resources" section). Global and regional business cases are available, which showcase the uplift in authentication success rate, approval rate, frictionless rate and fraud detection rate.

Will there be rules or non-compliance assessments for the newly required EMV 3DS data fields?

- The updated data fields outlined above will be required **effective 12 August 2024** as part of the *Visa Secure Program Guide*, which is a Visa Supplemental Requirements document. Merchants and acquirers will be required to support these minimum data requirements or request appropriate waivers, providing appropriate legal documentation if needed.

- While Visa is not planning to assess a fee at this time, merchants and acquirers are subject to a general rule that non-compliance assessments may occur based on monitoring findings (Visa Rules ID#: 0000482). In the event Visa decides to apply additional integrity fees related to these required data fields, clients will be notified in advance.

Will EMV 3DS transaction processing be impacted by non-compliance with the data field requirements?

- Transaction processing will not be impacted at this time. However, the data field requirements are a Visa Secure program requirement, which is supplemental to the Visa Rules. Per the Visa Rules (ID #: 0000385), merchants are required to meet the requirements, unless a regional / country regulation prohibits them from doing so. If a merchant is unable to comply, the merchant must appropriately request a waiver with a business justification to eventually comply; in this case, acquirers will need to work with their Visa representative to review the merchant's request and complete the form accordingly to process the waiver.

Can a merchant request an extension to the deadline?

- Visa has already provided a six-month advance notice from the original announcement made in AI13277 in the 31 August 2023 edition of the *Visa Business News*, in addition to a six-month extension to **12 August 2024** as announced in this article.

- **Note:** The data fields listed were already part of the specifications and were conditionally required, with the condition that the acquirer / merchant shall send this information to comply with any country / regional requirements.

Can a merchant provide null or spam (static) values to satisfy these data field requirements?

- Merchants should collect and provide true cardholder data in their AReq. Null / spam / static values will not support issuers in making accurate authentication decisions, and merchants should not provide these values in place of true cardholder data in their AReqs.

Additional Resources

Documents & Publications

AI13277 - "Visa Secure Program Updates: 12 Data Fields Required for EMV 3-D Secure Minimum Data Requirements and Amendments to Visa Secure Disputes," *Visa Business News*, 31 August 2023

AI13192 - "Launch of Issuer 3DS Authentication Dashboard in Visa Analytics Platform," *Visa Business News*, 27 July 2023

Online Resources

Refer to the following documentation 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*

Visit the Visa Secure Services Library to see merchant data quality global and regional business cases in the VSS Library under Merchant Resources.

Visit the Visa Analytics Platform section at Visa Online.

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

For More Information

AP: 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.

---

confidential; and (iii) the Information is designated as "affects merchants" demonstrated by display of the storefront icon on the communication. You must ensure that a merchant receiving such Information maintains the confidentiality of such Information and discloses and uses it on a "need to know" basis and only in their capacity as a participant in the Visa payments system. Except as otherwise provided herein or pursuant to applicable Confidentiality Restrictions, 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. The Information is provided "AS-IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa neither makes any warranty or representation as to the completeness or accuracy of the Information, nor assumes any liability or responsibility that may result from reliance on or use of such information. Please be advised that the Information may constitute material non-public information under U.S. federal securities laws and that purchasing or selling securities of Visa while being aware of material non-public information would constitute a violation of applicable U.S. federal securities laws. Participation in services is subject to Visa's terms and conditions in program participation agreements and associated documentation.

Benefits are illustrative only and depend on business factors and implementation details. The trademarks, logos, trade names and service marks, whether registered or unregistered (collectively the "Trademarks") are Trademarks owned by Visa. All other Trademarks not attributed to Visa are the property of their respective owners, are used for illustrative purposes only and do not imply product endorsement or affiliation with Visa unless the Information indicates otherwise. Capitalized terms not otherwise defined herein have the meanings given to them in the Visa Core Rules and Visa Product and Service Rules.