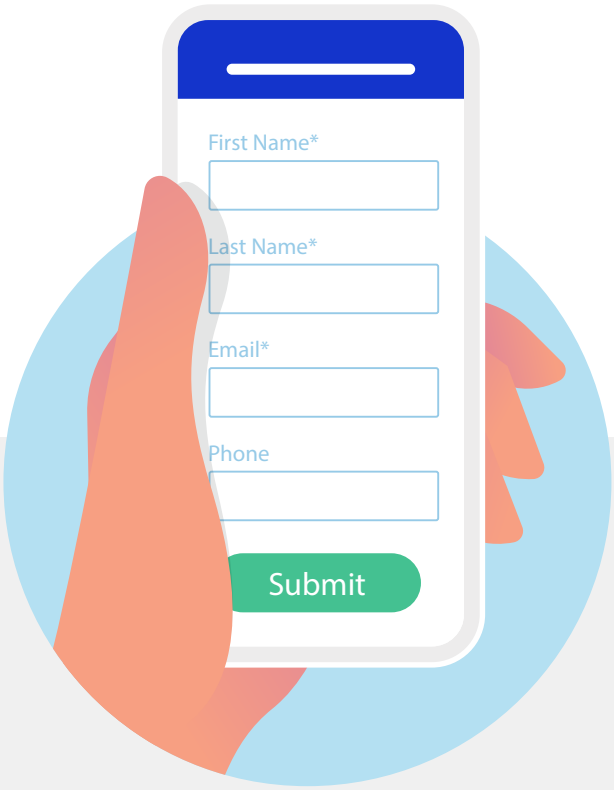
Minimum Data Requirements for Merchants

Merchants must provide the data elements in EMV 3DS authentication message (AReq) as follows:

Required always **Required conditional**

(Please refer to the Visa Secure Program Guide for a complete list of required, required conditional, and optional data elements.)



Data Element Categorization:

Message Inclusion

- **R** = Required
- **C** = Required Conditional
- **O** = Optional

Device Channel

- **A** = App
- **B** = Browser
- **3** = 3RI

Merchants are required to invoke the 3DS Method URL every time one is present for an Issuer. The Method URL allows Issuers to obtain additional device data that helps them make better decisions.

Merchants should launch the 3DS Method URL as early as possible in the checkout process. This will be driven by how soon they know which card is being used. As soon as the payment card is identified, the URL should be invoked.

Merchants should provide as much data as possible (including required, conditional, and optional data elements). Issuers use this data to analyze the risk of the transaction, which can reduce the number of challenges that occur.

Merchants should ensure that the data sent into authorization is accurate and consistent with the data sent into authentication. Providing EMV 3DS data is subject to regional and country regulations.

Top 4 Common Data Mistakes that Issuers Find from Merchants

Issuers are finding value in enhanced data from merchants. However, it is likely that some of the fields that are not currently being populated could greatly improve results.

Billing/Shipping Data Inconsistency

Not every country has the same naming convention (i.e., some regions have provinces, states, territories). Whenever possible, merchants should use a dropdown feature to improve accuracy and reduce human error in manually entered data

Raw data needs to be normalized where possible

I.e., Billing/Shipping address Line 1 would provide more value if in a standardized format rather than what was directly entered by the consumer

Derived values are showing promise in detecting fraudulent transactions

ID Information such as IP Address, Phone, etc. do not have past fraudulent transactions associated

Screen sizes are in a typical range (i.e., not 1px by 1px, etc.)

Device location relative to Billing or Shipping address

Data Inconsistency

Merchants should use card-on-file and consumer pre-filled data to ensure consistent entries for returning customers. This also improves consumer experience as the checkout process will be faster

Merchants should be aware that there are 2 types of data:

Systemic data

is captured automatically by the system (i.e., transaction amount, IP address and device)

Manually entered data

is captured through customer input fields

Customer input fields have a higher rate of error due to the nature of human error when manually entering data. Ensuring the use of drop-down menus and availability of card-on-file capabilities can greatly reduce error rates by minimizing customer input requirements.

Most Highly Rated as Effective Data Fields

Based on industry feedback, the following fields have been rated by multiple issuers as being either "Highly Effective" or "Useful".

Address Match Indicator
(addrMatch)

Cardholder Account Information
(acctInfo)

Cardholder Account Number
(acctNumber)

Browser IP Address
(browserIP)

Browser Screen Height
(browserScreenHeight)

Browser Screen Width
(browserScreenWidth)

Cardholder Name
(cardholderName)

Cardholder Billing Address City
(billAddrCity)

Cardholder Billing Address Country
(billAddrCountry)

Cardholder Billing Address Line 1
(billAddrLine1)

Cardholder Billing Address Line 2
(billAddrLine2)

Cardholder Billing Address Postal Code
(billAddrPostCode)

Cardholder Billing Address State
(billAddrState)

Cardholder Home Phone Number
(homePhone)

Cardholder Mobile Phone Number
(mobilePhone)

Cardholder Work Phone
(workPhone)

Cardholder Shipping Address City
(shipAddrCity)

Cardholder Shipping Address Country
(shipAddrCountry)

Cardholder Shipping Address Line 1
(shipAddrLine1)

Cardholder Shipping Address Line 2
(shipAddrLine2)

Cardholder Shipping Address Postal Code
(shipAddrPostCode)

Cardholder Shipping Address State
(shipAddrState)

Device Information
(deviceInfo)

Device Channel
(deviceChannel)

Merchant Country Code
(merchantCountryCode)

Merchant Name
(merchantName)

Merchant Risk Indicator
(merchantRiskIndicator)

Merchant Data Quality Best Practices to Improve Authorization Rates

Merchants should avoid overwriting blank fields with generic data. It is better to present blank fields than to provide fake merchant IDs or pre-filled data. When pre-filled or generic data (spam) is provided, this leads to a negative impact on the issuer's risk model, rule set and final risk decision.

Reasons why this has a negative impact:

1. It is not the consumer's true data, which leads to false assumptions
2. Repeated, pre-filled data fields result in significant elevation of velocity risk triggers in the issuer's risk model and rule set
3. Generic, pre-filled field entries hamper the ability of issuers' risk models to identify true fraud activity

VISA