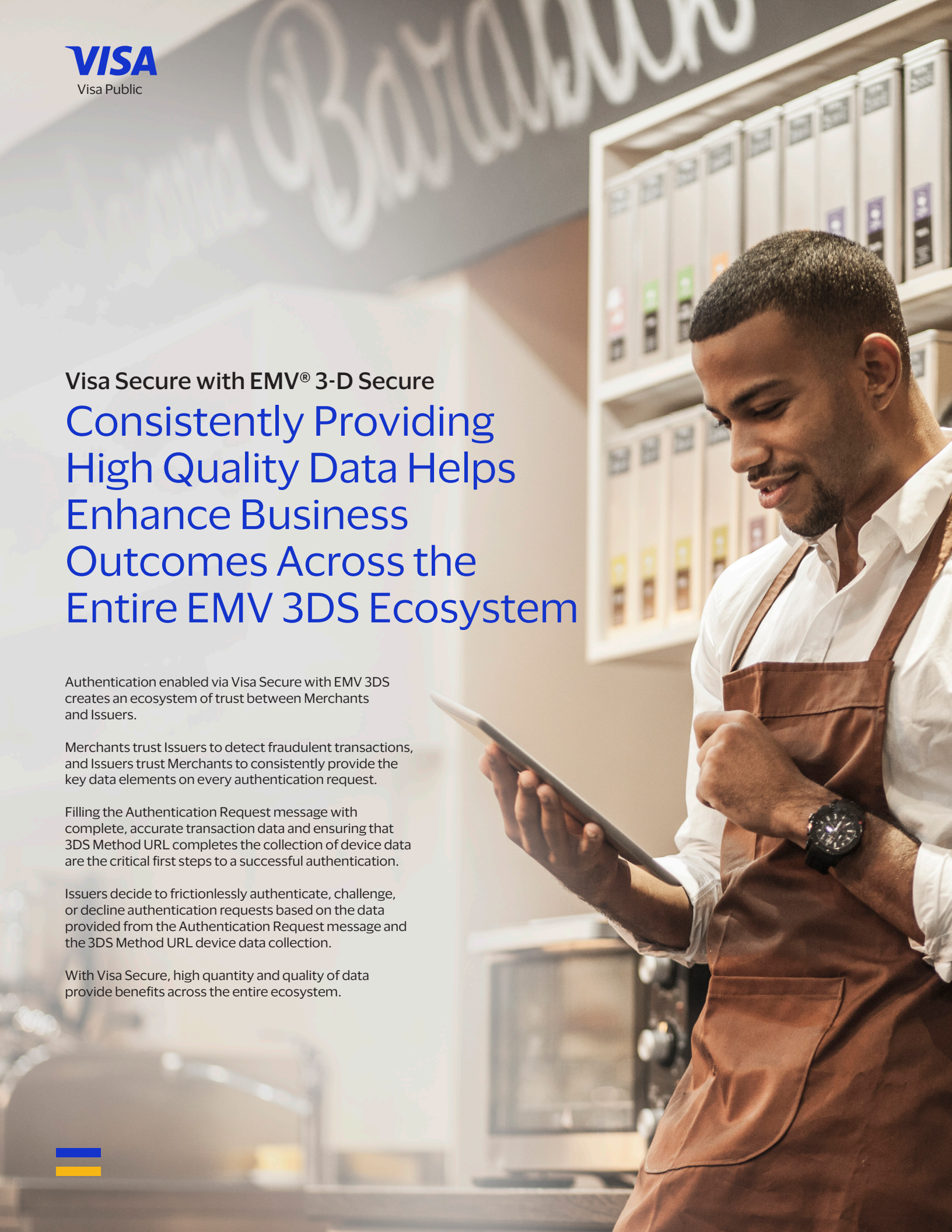


Visa Secure with EMV® 3-D Secure

Consistently Providing High Quality Data Helps Enhance Business Outcomes Across the Entire EMV 3DS Ecosystem

Authentication enabled via Visa Secure with EMV 3DS creates an ecosystem of trust between Merchants and Issuers.

Merchants trust Issuers to detect fraudulent transactions, and Issuers trust Merchants to consistently provide the key data elements on every authentication request.

Filling the Authentication Request message with complete, accurate transaction data and ensuring that 3DS Method URL completes the collection of device data are the critical first steps to a successful authentication.

Issuers decide to frictionlessly authenticate, challenge, or decline authentication requests based on the data provided from the Authentication Request message and the 3DS Method URL device data collection.

With Visa Secure, high quantity and quality of data provide benefits across the entire ecosystem.

Merchants

To realize the full benefits of Visa Secure authentication, Merchants are encouraged to provide the priority data elements in their Authentication Requests, and to invoke the 3DS Method URL and allow it to complete collection of device data.

On average, Merchants that c**omplete 3DS Method URL at least 95% of the time** see an **authentication success rate lift of 8%**, and **approval rate lift of 8%**, compared to Merchants with lower 3DS Method URL completion rates.[1]

↑ **8%** **Authentication Sucess Rate Lift**

↑ **8%** **Approval Rate Lift**

On average, Merchants that **populate more than 50% of the priority data elements** see an **authentication success rate lift of 4%,** and **approval rate lift of 6%,** compared to Merchants with lower population of priority data elements.[2]

↑ **4%** **Authentication Sucess Rate Lift**

↑ **6%** **Approval Rate Lift**

Cardholders

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

On average, Merchants that **complete 3DS Method URL at least 95% of the time** see a **frictionless rate lift of 127%** compared to Merchants with lower 3DS Method URL completion rates.[1]

↑ **127%** **Frictionless Rate Lift**

On average, Merchants that **populate more than 50% of the priority data element**s see a **frictionless rate lift of 57%** compared to Merchants with lower population of priority data elements.[2]

↑ **57%** **Frictionless Rate Lift**

[1]The dataset for these calculations contains 95+% of Visa Secure global transactions that occurred during the months of February through March of 2022. The uplift figures were generated by grouping Visa Secure Merchants based on their 3DS Method URL completion rate and averaging their product performance.

[2]The dataset for these calculations contains 95+% of Visa Secure global transactions that occurred during the months of February through March of 2022. The uplift figures were generated by grouping Visa Secure Merchants based on the rate at which they populate our priority data elements and averaging their product performance.

Issuers

Issuers use Risk Based Authentication (RBA) to analyze transactional data provided by the Merchant. RBA assesses the risk level to inform the next action required for authentication.

Merchants who provide the priority data elements and true cardholder information will help Issuers' RBA solutions to consistently produce accurate results and optimize authentication outcomes.

When priority data elements are included in the Merchant's authentication request, Issuers can see up to a **65% fraud detection rate lift** than when the data elements are missing.[3]

↑65% **Fraud Detection Rate Lift**

When transaction data is provided it helps ensure:

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

Issuers can expect excellent fraud-to-sales ratios, reduced cardholder challenges, and fewer customer service cases required.

Priority Data Elements

The following data elements have been found to be most useful for the performance of EMV 3DS.

Conditionally Required Data Fields

The EMV 3DS specification defines some data fields as "Conditionally required". The Merchant **must** include these conditional data elements in the Message if the Conditional Inclusion requirements are met (e.g., provide shipping address when goods are delivered). Note, this requirement does not apply if there are local data privacy regulations that prohibit sharing the data element.

Browser IP Address**	**Cardholder Billing Address Postal Code**	**Cardholder Shipping Address Country**
Browser Screen Height**	**Cardholder Billing Address State**	**Cardholder Shipping Address Line 1**
Browser Screen Width**	**Cardholder Email Address**	**Cardholder Shipping Address Postal Code**
Cardholder Billing Address City	**Cardholder Name**	**Cardholder Shipping Address State**
Cardholder Billing Address Country	**Cardholder Phone Number**	**Common Device Identification Parameter***
Cardholder Billing Address Line 1	**Cardholder Shipping Address City**	

* IP Address for SDK transactions **Browser-only data fields

Optional Data Fields

Optional data fields are not required for authentication requests with Visa Secure. However, it is a best practice to include these fields when available to maximize the benefits of EMV 3DS.

Address Match Indicator	**Cardholder Account Information**

[3]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 RBA model.

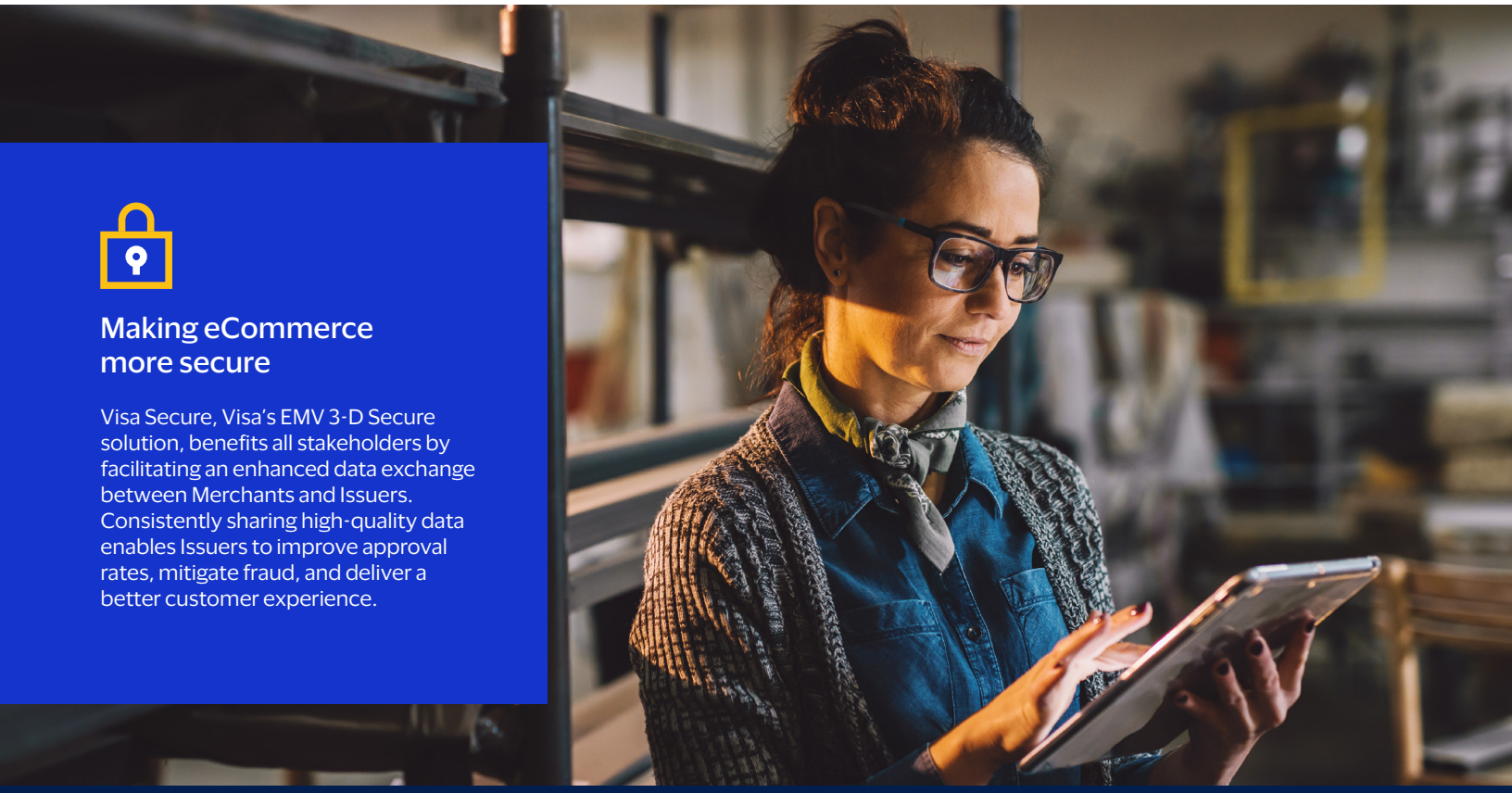
3DS Method URL

Enablement of the 3DS Method URL allows the Issuer to collect browser information and device fingerprint data before the authentication request is initiated by a Merchant.

3DS Servers should wait 5 seconds for the Method URL to complete. If the Method URL is not completed before a Merchant sends in an authentication request, then this results in missing browser information or device data. 3DS Servers shall set the 3DS Method Completion Indicator = Y upon notification from the 3DS requestor. If the 3DS method does not complete within 5 seconds, set the Method Completion Indicator to = N.

Merchant Data Quality Best Practices

1. Investigate whether the checkout page is designed to collect the required and priority EMV 3DS data elements, and take actions to populate any missing data fields.
2. Ensure that data sent through EMV 3DS is authentic and accurate at the time of the transaction.
3. Ensure that the 3DS Method URL is invoked and completed before sending an authentication request.



Making eCommerce more secure

Visa Secure, Visa's EMV 3-D Secure solution, benefits all stakeholders by facilitating an enhanced data exchange between Merchants and Issuers. Consistently sharing high-quality data enables Issuers to improve approval rates, mitigate fraud, and deliver a better customer experience.

Contact your Visa representative to learn more about Visa Secure with EMV 3DS or to request a demo.