E-Commerce & Authentication   4 February 2021

Visa Will Discontinue Support of 3-D Secure 1.0.2

Global | *Acquirers, Issuers, Processors, Agents*
Visa, Interlink, Plus Networks; V PAY; Europe Processing

Overview: Effective 15 October 2022, Visa will discontinue support of 3-D Secure 1.0.2 and related technology.

Visa Secure is designed to make online payments more secure by enabling an issuer to authenticate its cardholders, thus ensuring payments are made by the legitimate owner of the account. 3-D Secure (3DS) is the specification that defines the messages and data that enable the authentication to occur. 3DS 1.0.2 is the original version of the specification that was introduced over 15 years ago. An updated version of the specification, EMV® 3DS, was published in October 2016, and provides for a seamless user experience, enhanced data exchange for better fraud management and authorization decision making, and support across multiple payment channels and devices.

> **Mark Your Calendar:**
> - Visa will discontinue support of 3DS 1.0.2 Attempts Server **(16 October 2021)**
> - Visa will discontinue support of 3DS 1.0.2 **(15 October 2022)**

Visa is committed to supporting the industry's transition from 3DS 1.0.2 to EMV 3DS; therefore, **effective 15 October 2022**, Visa will discontinue support for 3DS 1.0.2 and all related technology.

To give clients more time to prepare for the full sunset of 3DS 1.0.2, Visa has decided to revise the rule change that was announced in the 16 April 2020 edition of the *Visa Business News* to remove merchant fraud liability protection on 3DS 1.0.2 transactions.

Effective 16 October 2021, Visa will continue to support 3DS 1.0.2 transaction processing, including the 3DS 1.0.2 Directory Server (DS), but will stop support of 3DS 1.0.2 Attempts Server for non participating issuers. After 15 October 2021, Visa will respond with a Verify Enrollment Response (VERes) = N to all authentication requests when the issuer does not support 3DS 1.0.2 (e.g. BIN range does not have an access control server [ACS] URL listed in the DS).

If an issuer continues to support 3DS 1.0.2 after 15 October 2021, it will be able to respond to merchants with a fully authenticated response and Cardholder Authentication Verification Value (CAVV), and merchants will obtain fraud liability protection. These transactions will be blocked from fraud-related disputes[1] in Visa Resolve Online. Issuers wishing to stop support of 3DS 1.0.2 must request that their Bank Identification Number (BIN) ranges be removed from the Visa Secure DS.

Visa Secure Using 3DS 1.0.2	Prior to 16 October 2021	Beginning 16 October 2021
Fully authenticated (Issuer participates)	Fraud liability with issuer (Electronic Commerce Indicator [ECI] 05)	No change

Attempted authentication (Issuer participates and ACS is unavailable or respons VERes = N)[2]	Fraud liability with issuer (ECI 06)	No change
Attempted authentication (Issuer does not participate)	Fraud liability with issuer (ECI 06)	Fraud liability with merchant (ECI 07)

Re-enabling the 3DS 1.0.2 Card Range Message Pair

For merchants to determine which issuers continue to support 3DS 1.0.2 after 15 October 2021, Visa will re-enable the Card Range Request (CRReq) and Card Range Response (CRRes) messages for 3DS 1.0.2 that had been previously disabled. Merchant server plug-ins (MPIs) can send the CRReq / Res message to the Visa Secure 3DS 1.0.2 DS, and a list of all issuer BIN ranges participating in 3DS 1.0.2 will be returned. Providers of MPIs will need to make updates to include the use of these messages.

 Note: There will be no changes to the Visa Secure EMV 3DS rules.

[1] Fraud-related disputes include Dispute Condition 10.4.

[2] The Visa Attempts Server will continue to stand in.

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

For More Information

Merchants and third party agents should contact their acquirer.