

Strong Customer Authentication: Communication on improving outcomes from 3DSecure – Data Consistency

Date: 2 July 2020

This document is being issued to help assist merchants, gateways and web service content management providers with the implementation of 3DSecure and follows on from our [previous communication on 28 January 2020](#).

Who is this communication for?

This document is aimed at merchants, gateways and web service content management providers using or in the process of implementing 3DSecure version 2 or higher.

Why does it matter to you?

There have been common errors which are causing declines in the data consistency of 3DSecure transactions. This guidance helps merchants and their technology partners to achieve the benefit of optimised checkout experience, in other words, a greater number of successful transactions.

What should you do?

Merchants, gateways and content management providers need to review their e-commerce data capture configurations, such as on websites and apps, and adopt the guidance as appropriate

Executive summary

Merchant support of 3DSecure (3DS)¹ is very important in ensuring readiness for online transactions and avoiding declines after Strong Customer Authentication (SCA) is live in the UK before **14 September 2021**. Merchants should be ready by **May 2021** when payment service providers (PSPs) will begin randomly checking SCA compliance and declining transactions that are non-compliant.

Before that point, merchants must decide which version of 3DS they require to meet their compliance needs: version 1, version 2.1, or version 2.2.

3DS v2.1 or v2.2 is recommended due to its ability to reduce friction at checkout compared to v1. However, its benefit over 3DS v1 is not currently being realised due, primarily, to poor data quality/consistency for data fields which are new to v 2. This guidance aims to provide clarity and best practice for these data usages.

¹ Please refer to the UK Finance Communication on Strong Customer Authentication for further information

3D Secure supports card transactions for e-commerce but there are alternative solutions available, such as sending transactions directly to authorisations with the correct flag and payments made through Open Banking and other app-based solutions

What is happening today?

Transactions sent via 3DS v2 are currently experiencing higher step-up/challenge rates than 3DS v1. Inconsistency for some data fields has caused issuers' fraud checks to falsely identify these transactions as fraud.

Investigations, led by UK Finance, have identified **three key data fields** which have caused a significant number of errors with 3DS v2. Merchants, gateways or content management providers must capture and submit this data correctly to avoid declines.

Key Findings² – 3DSv2 data consistency

- The 3DS method URL:** This helps recognition of the browser and device and is not being used by merchants – around 30 per cent of transactions sampled did not have this data.
- Three key fields:** as detailed in the below table, are either missing, incomplete or inaccurate – observed in 30-80 per cent of transactions sampled.
- Remaining Fields:** Other optional but useful data fields can also improve the challenge rates.

ID	Title	Volume*	Action	Comments
1	3DS Method	~30%	Call the 3DS method url when authenticating	<ul style="list-style-type: none"> The 3DS method url enables the ACS to recognise the browser device This is considered essential This information also allows for recognition returning customers.
2	Key Fields	<ol style="list-style-type: none"> ~30% ~40-70% ~50-80% 	Aside from the Mandatory fields, completing all of the below: <ol style="list-style-type: none"> Browser IP (field 21) Shipping & Billing Post code (fields 11 & 26) Address match indicator (Field 27) 	<ul style="list-style-type: none"> Field 21: The publicly routable customer browser IP is essential to the correct operation of the protocol Field 11 & 26: The inclusion of the first half of the UK post code as a minimum is essential, even better with the full post code Field 27: It is recommended to use address validation. However if merchants are unable to send the full address, information in field 27 provides anonymous indicator to improve accuracy of risk assessment In the case of 'electronic shipping', the address is expected to be blank (delivery/timeframe = electronic shipping)
3	Remaining Fields	~70-100%	As a general rule the completion of as many fields as possible will always help to reduce challenge rates over time. As it will help with the learning of Merchants trends	<ul style="list-style-type: none"> In a SCA environment, the merchant provision of more fields consistently and accurately may increase effectiveness of the issuer TRA exemption (Issuer's TRA exemption threshold is based on their fraud ratios) Some relevant fields include: merchantName, MCC, acquirerMerchantID,

*Volume of 3DS v2 web browser transactions with missing / inaccurate

- ² Findings and recommended actions have been reviewed with Scheme, Gateway, and Merchant representatives in preparation of this guidance.

Recommendations

Merchants

- If you are already using 3DS v2 - review how you currently capture the data relevant to 3DS v2 data capture and the submissions to address. You should aim to address these errors as soon as possible.
- If you are yet to adopt 3DS v2 - please apply this guidance as you move towards implementation to avoid these issues.

Acquirers/gateways/web service content management/Enterprise Resource Planning (ERP) providers

- We recommend that you incorporate this guidance into merchant configuration and testing where applicable.
- It is also recommended that you incorporate this in your communications and guidance to merchants to support their implementations.

Testing Considerations

It is important to remember that when SCA is being tested or on go-live, the following general rules will apply:

- Challenge rates are expected to be higher for all versions of 3DS as all transactions without an SCA exemption or those out of scope will need to be authenticated as a default position.
- Challenge rates for 3DS v2.2 (or v2.1 with extensions) are expected to be lower than 3DS v2.1 and v1 as it allows the additional option to apply an acquirer exemption: transaction risk analysis.

Next steps

- UK Finance will be monitoring 3DS v2 outcomes periodically and partner with ACS providers to undertake a quarterly review of progress.
- Further assessments are planned to review the performance of 3DS v2 (particularly in an app context) once volumes start to increase. Further guidance may be issued if needed.