Preventing EMV® 3DS to 3DS 1.0.2 Downgrades

The sunset of 3DS 1.0 is **coming this October.** When the sunset occurs, the Directory Server will no longer be able to support 3DS 1.0 transaction requests, and Cardinal will sunset 3DS 1.0 and all its features (except in countries with network extensions).

Pre-Sunset

The networks currently support both 3DS 1.0 and EMV 3-D Secure. Today, when a transaction comes into Cardinal, and it does not contain the required information to support an EMV 3DS transaction, the transaction is routed down 3DS 1.0. This routing prevents the transaction from failing authentication, maintains PSD2 SCA (Strong Consumer Authentication) compliance, and retains liability protection for those transactions that are authenticated by the issuer.

Post-Sunset

After the sunset, these transactions can no longer be routed down 3DS 1.0. Instead, the transactions will have an unauthenticated outcome. This means that they will not be PSD2 compliant, and the merchant will not receive liability protection.

About this document

This error description document outlines several scenarios where a transaction currently gets routed down 3DS 1.0, when it does not contain the required information to be eligible for EMV 3DS processing. To maintain PSD2 compliance and receive liability protection, it is important to pay attention to these downgraded transactions. If these situations occur on or after the sunset date in October, then the transaction will result in an unauthenticated outcome and will not route down EMV 3DS.

Please work with your Customer Success Manager if needed. If you are unsure of who that is, please contact support@cardinalcommerce.com. For additional information on the sunset, visit http://www.cardinalcommerce.com/sunset.

The matrix below outlines downgrade types, reasons, and mitigation plans:

Types	Downgrade Reasons	Mitigation Plan
1	Missing required field on Lookup Request; **DFReferenceId*** (DFReferenceID not present)	**What this means:** DFReferenceId* field is required to be passed by the merchant on the Lookup Request. This allows Cardinal to link browser fields collected during the Device Data Collection (DDC) call and indicate the outcome of the 3DS Method call on the Authentication request. **What to do:** 1. Ensure you are running Device Data Collection. 2. Proceed with Lookup Request after Device Data Collection completes. 3. Make sure you are sending the DFReferenceID* on the Lookup Request that you received on the Device Data Collection. 4. As a backup, make sure you are sending 11 browser fields on the Lookup Request. 5. If you need additional information, please reference our Device Data Collection page.
2	Version 1.0 sent on Lookup Request (Merchant Version Preference)	**What this Means:** Merchants are passing ThreeDSVersion = 1.0 on the Lookup request. **What to Do:** 1. Remove ThreeDSVersion from your Lookup API request – Cardinal will route the transaction to the highest supported version. 2. If you do not know how to do this, please contact your Customer Success Manager. 3. If you are unsure of who your Customer Success Manager is, please contact support@cardinalcommerce.com.

Types	Downgrade Reasons	Mitigation Plan
3	Merchant initiated Lookup Request before completing Device Data Collection (Missing V2 Required Fields)	**What this means:** Data collection needs to be completed before a merchant can initiate the Lookup request. **There are several instances where this can occur:** 1. DeviceChannel not present 2. Partial browser fields collected on DDC 3. Merchant did not run DDC **What to do:** 1. Ensure you are running Device Data Collection. 2. Proceed with Lookup Request after Device Data Collection completes. 3. Make sure you are sending the DFReferenceID* on the Lookup Request that you received on the Device Data Collection. 4. As a backup, make sure you are sending 11 browser fields on the Lookup Request. 5. If you need additional information, please reference our Device Data Collection page.
4	Cardinal Merchant ID not configured for EMV 3DS (EMV 3DS Config Not Enabled)	**What this means:** You must migrate to EMV 3DS prior to the October sunset of 3DS 1.0. **What to do:** 1. Please contact your Customer Success Manager to configure your account to process EMV 3DS transactions. 2. If you are unsure of who your Customer Success Manager is, please contact support@cardinalcommerce.com.
5	Rules downgraded the transaction to 1.0 (Rules forced transaction to 1.0)	**What this means:** There is a rule in place that is downgrading transactions to 3DS 1.0. After the October sunset, transactions downgraded to 3DS 1.0 will result in an unauthenticated outcome. **What to do:** 1. Please contact your Customer Success Manager to configure your account to process EMV 3DS transactions. 2. If you are unsure of who your Customer Success Manager is, please contact support@cardinalcommerce.com.

Types	Downgrade Reasons	Mitigation Plan
6	3DS 1.0 Replay (3DS2 Replay - EnrollmentU, 3DS2 Replay - Attempts, 3DS2 Replay - Identity Check, 3DS2 Authentication Unavailable at ACS) Note 1: The above is applicable only in certain use cases. If you are not using the 3DS 1.0 Replay functionality, this does not apply to you. Note 2: Cardinal will be deactivating the Replay functionality for all transactions in alignment with 3DS 1.0 Sunset dates (with the exception of intraregional transactions in India).	**What this means:** There is a configuration in place to replay EMV 3DS transactions down 3DS 1.0 in certain scenarios. **There are two instances where this can occur:** 1. Replay Attempts: Replay re-runs the transaction down 3DS 1.0 instead of allowing an EMV 3DS attempts. 2. Replay Enrollment U: Indicates replay occurred on the transaction and the transaction was downgraded to 3DS 1.0. This happens when there is an error or problem processing an EMV 3DS transaction. **What to do:** 1. If you are using the 3DS 1.0 Replay functionality, please contact your Customer Success Manager to configure your account to process EMV 3DS transactions. 2. If you are unsure of who your Customer Success Manager is, please contact support@cardinalcommerce.com. 3. If you are not using the 3DS 1.0 Replay functionality, you do not need to do anything.

*For reference, below is more information on the DFReferenceID:
ConsumerSessionId returned upon the completion of Device Data Collection call is required to be passed by the merchant as "DFReferenceId" on the Lookup Request in order for Cardinal to facilitate the linkage of browser fields collected during the Device Data Collection (DDC) call and indicate the outcome of the 3DS Method call on the Authentication request (AReq) during an EMV 3DS transaction.