Merchant-Initiated Transactions & Stored Credentials Mandates

FAQ for Merchants Using CyberSource Tokenization[1]

What are the mandates?

The mandates aim to provide more information to issuers and cardholders about transactions initiated by merchants, and about payment credentials that are stored by or on behalf of merchants.

At a high level:

- Cardholder consent is required to store card details on file.
- All transactions based on credentials on file need to be marked as such.
- All merchant-initiated transactions need to link to a previously successful authorization.
- The reason for merchant-initiated transactions needs to be provided.

Why should I care?

Compliance should result in improved authorization success rates for transactions that:

- are follow-on transactions initiated by merchants—*such as recurring or subscription payments*

and/or

- use payment credentials that are stored on file—*such as one-click checkout experiences based on CyberSource Tokenization*

Compliant merchants will also be able to enroll in the Real Time Visa Account Updater service when it becomes available. This service enables merchants to get updated card information as part of the authorization message in real time. Receiving that real-time information reduces the number of declines for authorizations with stored credentials due to expired, lost, or stolen cards.

What do I need to do?

If you are using CyberSource's Tokenization or Recurring Billing services, we will handle most of the complexity for you. If you are not using Tokenization, you should consult the general MIT and Card on File FAQ or speak to your CyberSource account manager about the benefits of implementing tokenization.

Consult the checklist below to see if you need to perform any actions to become compliant and put in place a plan to avoid unnecessary card authorization declines.

Checklist for compliance for merchants using CyberSource Tokenization or Recurring Billing

[1] This document applies to Cybersource's Token Management System (TMS) and merchants using the legacy Secure Storage (SS) solution

☑ When creating a payment token, ensure you gain the consent of the cardholder to store their payment details.

☑ When creating a token, try to carry out an authorization with step-up challenge indicator set for 3DS.

- Your first authorization using the token should contain the following fields and values:

SCMP	SO API	REST
subsequent_auth_first = "Y"	subsequentAuthFirst = true	processingInformation. authorizationOptions. initiator.credentialStoredOnFile==true
pa_challenge_code = 04	payerAuthEnrollService_challengeCode= 04	consumerAuthenticationInformation. challengeCode=04

☑ Review your use of tokens, which should fall into one or more of the following categories:

Category	Description	Action required
Customer Initiated	A customer actively initiates a transaction using a token you have stored against his or her account. For example: One-click checkout.	**None.** CyberSource will automatically mark the transaction as a credential on file.
Recurring	A series of transactions, processed at fixed, regular intervals for a fixed amount, no more than annually. The eCommerce indicator is set to recurring.	**None.** CyberSource will automatically mark the transaction as a credential on file, and link to a previously successful authorization using that card.
Installment	A single purchase of goods or services billed to a cardholder in multiple transactions over a period of time agreed to by the cardholder and merchant. The eCommerce indicator is set to install.	**None.** CyberSource will automatically mark the transaction as a credential on file, and link to a previously successful authorization using that card.
Unscheduled Card on File	A merchant-initiated transaction using a stored credential for a fixed or variable amount that does not occur on a scheduled or regularly occurring transaction date. For example, an auto-top up of a travel card. The eCommerce indicator is set to internet.	Add the following to Auth request: **SCMP:** subsequent_auth = "Y" **SOAPI:** subsequentAuth = true **REST:**

		processingInformation. authorizationOptions.initiator.type = merchant CyberSource will automatically mark the transaction as an unscheduled credential on file, and link to a previously successful authorization using that card.
Resubmission	A token is used to resubmit an authorization previously declined due to insufficient funds, where the goods or services have been delivered to the cardholder. The eCommerce indicator is set to internet.	Add the following to Auth request: **SCMP:** subsequent_auth = "Y" subsequent_auth_reason = "1" **SOAPI:** subsequentAuth = true subsequentAuthReason = 1 **REST:** processingInformation. authorizationOptions.initiator.type = merchant processingInformation. authorizationOptions.initiator. merchantInitiatedTransaction.reason = 1 CyberSource will automatically mark the transaction as a credential on file, and link to a previously successful authorization using that card.
Delayed Charges	A supplemental account charge processed after original services have been rendered and respective payment has been processed.	Add the following to Auth request: **SCMP:** subsequent_auth = "Y" subsequent_auth_reason = "2" **SOAPI:** subsequentAuth = true subsequentAuthReason = 2 **REST:**

		processingInformation. authorizationOptions.initiator.type = merchant processingInformation. authorizationOptions.initiator. merchantInitiatedTransaction.reason = 2 CyberSource will automatically mark the transaction as a credential on file, and link to a previously successful authorization using that card.
Reauthorization Charges	A merchant initiates a reauthorization when the completion or fulfillment of the original order or service extends beyond the authorization validity limit set by the scheme. For example, split shipments.	Add the following to Auth request: **SCMP:** subsequent_auth = "Y" subsequent_auth_reason = "3" **SOAPI:** subsequentAuth = true subsequentAuthReason = 3 **REST:** processingInformation. authorizationOptions.initiator.type = merchant processingInformation. authorizationOptions.initiator. merchantInitiatedTransaction.reason = 3 CyberSource will automatically mark the transaction as a credential on file, and link to a previously successful authorization using that card.
No Show Charge	Cardholders can use their cards to make a guaranteed reservation with certain merchant segments. A guaranteed reservation ensures that the reservation will be honored and allows a merchant to perform a no-show transaction to charge the cardholder a penalty according to the merchant's cancellation policy.	Add the following to Auth request: **SCMP:** subsequent_auth = "Y" subsequent_auth_reason = "4" **SOAPI:** subsequentAuth = true subsequentAuthReason = 4

	For merchants that accept token-based payment credentials to guarantee a reservation, it is necessary to perform a CIT (Account Verification Service) at the time of reservation to be able to perform a no-show transaction later.	**REST:** processingInformation. authorizationOptions.initiator.type = merchant processingInformation. authorizationOptions.initiator. merchantInitiatedTransaction.reason = 4 CyberSource will automatically mark the transaction as a credential on file, and link to a previously successful authorization using that card.