FAQ
Visa Merchant Initiated Transactions & Stored Credentials Mandates

What’s the important news?

1. Visa introduced a new framework for Merchant Initiated Transactions (MIT) to identify transaction intent and cardholder participation in the transaction. Any transaction initiated by merchant as a follow on to an initial Cardholder Initiated Transaction must follow the MIT framework to benefit from higher authorization rates and successful processing of subsequent MIT’s.

2. Visa also announced requirements for its Stored Credentials framework, to identify initial storage and subsequent use of payment credentials by merchants. Following the authorization rules defined as part of the framework for all card on file (COF) transactions is expected to result in higher authorization approval rates. It also is required for merchants to benefit from participation in the Real Time Visa Account Updater. Real Time Account Updater service enables merchants to get updated card information as part of authorization message in real time.

**Key Takeaway:** Both mandates require merchants to upgrade their integrations with CyberSource.

This also applies to our commerce server integrations (cartridges, modules, plugins, etc.)

What can I do to keep up with these mandates?

Identify the scenarios applicable to your business and accordingly upgrade your integration with CyberSource. You can use the existing and new API fields that are described for different scenarios for both mandates as below to make sure your system is updated with the changes needed by the two mandates. As soon as your processor implements and communicates the changes made, CyberSource will update its connection and enable you to be fully compliant. The extra fields that you pass in the request while your processor isn’t yet ready to accept would be dropped by CyberSource and your transactions would continue to be processed as today.

Please refer to the attached Microsoft Presentation for examples of API requests for MIT and COF scenarios using the new and existing API fields.

**Merchant Initiated Transactions - MIT**

Does the MIT mandate require merchants to modify their CyberSource integrations?
Yes. Changes for MIT are mandated for only network token transactions at this time, though it is recommended merchants update for PAN transactions as well. Merchants are required to update their integration with CyberSource to comply with the framework. As the acquirers and processors get ready with the changes, CyberSource plans to update our connections enabling merchants to start leveraging the framework for a better authorization approval rate.

What are MIT’s?

Merchant-initiated Transaction (MIT): Merchants commonly initiate transactions without the active participation of the cardholder to:

- Perform a transaction as a follow-up to a cardholder-initiated transaction (CIT)
- Perform a pre-agreed standing instruction from the cardholder for the provision of goods or services

Examples of MITs include:

- A hotel charge for mini-bar expenses tallied after the guest has checked out and closed the folio
- A subsequent recurring payment for a magazine subscription

Digital payment made via an app to purchase goods or order services at customer’s request—such as ordering a ride or buying train tickets—are not MITs but are cardholder-initiated as the cardholder actively participates in them.

What problem does this MIT framework address?

Prior to the introduction of the MIT framework, it was not possible to identify transaction intent or the cardholder’s active participation. A merchant could initiate a transaction, but without the cardholder’s active participation, they could not provide some authentication elements—such as track data, cryptogram, or Card Verification Value 2 (CVV2)—to the issuer. Consequently, issuers often declined MITs.

Further, the introduction of payment tokens required authentication data elements (i.e., cryptogram) for every transaction. Merchants in these scenarios could not perform transactions when the cardholder was not actively participating, such as a reauthorization of a split shipment. In the absence of a standard framework these transactions failed, were declined, or in some instances were processed inconsistently across geographies.

How do merchants benefit from the MIT framework?
Higher authorization approval rates and sales conversions. MIT framework makes recurring & reauthorization scenarios more reliable with less likelihood of rejection. In case of payment token transactions, enables successful processing of subsequent MIT’s.

How?

The MIT framework:

• Introduces a global standard to identify transaction intent and whether a transaction is merchant-initiated—i.e., a cardholder is actively participating and available for authentication. It also enables merchants, acquirers, and issuers to link a series of related transactions together.

• Enables consistent MIT processing globally.

• Provides transaction transparency, resulting in higher authorization rates and improved cardholder experience.

• Allows merchant-initiated, token-based transactions to be processed without authentication data elements.

As MITs are performed as a follow-up to a cardholder-initiated transaction (CIT), merchants and acquirers accepting CITs with a payment token must comply with the MIT framework to enable successful processing of the subsequent MITs they perform. Merchants may accept payment tokens in CITs in some of the following scenarios:

• payWave transactions

• Online payments via digital wallets that use payment tokens

• Payment transactions from devices equipped with Magnetic Secure Transmission™ (MST) technology

What’s the impact on CyberSource Merchants?

The MIT construct is available for all transactions initiated by the merchant where the cardholder is not present. However, the changes for MIT are only mandated for network token transactions at this time. The framework being introduced will better allow merchant who have implemented any of the ‘Pay’ products, to handle complex payment scenarios that currently aren’t supported or have limited support.

Key Points:

• Changes are mandated for network token transactions.

• No changes to current network token processing rules have been put into effect at Visa, but we expect them to be made sometime in 2018.
• MIT framework makes recurring & reauthorization scenarios more reliable with less likelihood of rejection.

What changes to CyberSource integration do I make to comply with the mandate?

All MIT transactions must include the below data values defined by the framework, to comply with the mandate:

**Merchant initiated transaction indicator:** To identify a transaction as MIT the API field “subsequent_auth” needs to be included in the transaction.

**Transaction Identifier:** A transaction Identifier needs to be included in all MIT’s using ‘subsequent_auth_transaction_id’. For all Industry practice MIT scenarios, the transaction identifier of the original CIT needs to be included, whereas for all standing Instructions MIT scenarios, the transaction identifier of the previous transaction needs to be included.

**MIT Reason Code:** In order to identify the intent behind MIT, each MIT must include the appropriate reason code depending on the scenario using the API field ‘subsequent_auth_reason’. For resubmission, delayed charges, reauthorization, no-show, use reason codes 1, 2, 3 and, 4 respectively.

**Installment/Recurring transactions indicator:** There is no change in the way Installment or Recurring type of transactions are marked. They must continue to use API field ‘e_commerce_indicator’.

**Unscheduled card on file:** All transactions using card on file payment credentials must be marked using API field ‘subsequent_auth_stored_credentials’.

What’s the impact on CyberSource?

As this framework is rolled out and implemented by our acquirers and processors, CyberSource will be making updates to our connection interfaces to comply with the new specifications defined in support of MIT. Currently in order to comply with the mandate, a number of our processor and acquiring partners are in the process of updating their system to meet the October 2017 mandate. CyberSource connections will be upgraded based on the MIT implementation date on the processor systems, with priority going to those connections that support Network Tokens.

Key Points

• Processors & Acquirers are updating their systems to support MIT

• CyberSource is updating all its connections to support MIT
What are MIT Use Cases?

The MIT framework covers two types of MITs:
- Industry-Specific Business Practice MITs
- Standing Instruction MITs

**Incremental**: Incremental authorizations can be used to increase the total amount authorized if the authorized amount is insufficient. An incremental authorization request may also be based on a revised estimate of what the cardholder may spend. Incremental authorizations do not replace the original authorization—they are additional to previously authorized amounts. The sum of all linked estimated and incremental authorizations represents the total amount authorized for a given transaction. An incremental authorization must be preceded by an estimated/initial authorization.

One or more incremental authorizations can be requested while the transaction has not yet been finalized (submitted for clearing). Incremental authorizations must not be used once the original transaction has been submitted for clearing. In such a scenario, a new authorization must be requested, with the appropriate reason code (e.g., delayed charges, reauthorization).

**Resubmission**: A merchant performs a resubmission in cases where it requested an authorization, but received a decline due to insufficient funds; however, the goods or services were already delivered to the cardholder. Merchants in such scenarios can resubmit the request to recover outstanding debt from cardholders.
**Reauthorization**: A merchant initiates a reauthorization when the completion or fulfillment of the original order or service extends beyond the authorization validity limit set by Visa. There are two common reauthorization scenarios:

- Split or delayed shipments at eCommerce retailers. A split shipment occurs when not all the goods ordered are available for shipment at the time of purchase. If the fulfillment of the goods takes place after the authorization validity limit set by Visa, eCommerce merchants perform a separate authorization to ensure that consumer funds are available.
- Extended stay hotels, car rentals, and cruise lines. A reauthorization is used for stays, voyages, and/or rentals that extend beyond the authorization validity period set by Visa.

**Delayed Charges**: Delayed charges are performed to process a supplemental account charge after original services have been rendered and respective payment has been processed.

**No Show**: Cardholders can use their Visa 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.

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 perform a No Show transaction later.

**Installment Payments**: A transaction in a series of transactions that use a stored credential and that represent cardholder agreement for the merchant to initiate one or more future transactions over a period for a single purchase of goods or services.

**Recurring Payments**: A transaction in a series of transactions that use a stored credential and that are processed at fixed, regular intervals (not to exceed one year between transactions), representing cardholder agreement for the merchant to initiate future transactions for the purchase of goods or services provided at regular intervals.

**Unscheduled Credential on File (UCOF)**: A transaction using a stored credential for a fixed or variable amount that does not occur on a scheduled or regularly occurring transaction date, where the cardholder has provided consent for the merchant to initiate one or more future transactions. An example of such transaction is an account auto-top up transaction.

What resources are available to help merchants implement this MIT framework and where can I learn more?
CyberSource technical guide provides details on new API’s introduced by CyberSource to enable merchants comply with the mandate:
http://apps.cybersource.com/library/documentation/dev_guides/CC_Svcs_SCMP_API/Credit_Cards_SCMP_API.pdf

The resource center at https://www.cybersource.com/mitsc_mandate/ is the best place to start. Merchant Support is also available to help guide merchants through this change.

**Stored Credentials / Card on File Transactions**

**Does this require merchants to modify their CyberSource integrations?**

Yes. Merchants that offer cardholders the opportunity to store their payment credentials on file must:

- Utilize appropriate data values (i.e., Stored Credential indicators as per the Stored Credential Transaction Framework) to identify initial storage and subsequent usage of stored payment credentials.

As the acquirers and processors get ready with the changes, CyberSource plans to update our connections enabling merchants to start leveraging the framework for a better authorization approval rate.

**What are Stored Credentials?**

A Stored Credential is information (including but not limiting to, an account number or payment token) that is stored by a merchant or its agent, a payment facilitator or, a staged digital wallet operator to process future transactions. Any transaction where the payment details (PAN or DPAN) are not provided by the cardholder but are fetched from the merchant’s system is considered a Stored Credential transaction.

Payment credentials received by merchants from third parties including pass-through digital wallets that are not stored by the merchant, its agent, or PF are not considered stored credentials. For example, a payment credential received by a merchant on a purchase from Visa Checkout and not stored by that merchant, its agent, or PF is not considered a stored credential.

A credential is also not considered a stored credential when the merchant or its agent, PF, or SDWO stores the credential to complete a single transaction or a single purchase for a cardholder (including multiple authorizations related to that particular transaction). For example, when a cardholder provides a payment credential to a hotel to cover future reservations and charges as part of the cardholder’s membership profile, it is considered a
stored credential. However, when the cardholder provides the payment credential to a hotel to cover charges related to a specific reservation only, it is not.

**What problem does the Stored Credential framework address?**

Growth in digital commerce, together with the emergence of new business models, has increased the number of transactions where a merchant or its agent, a payment facilitator (PF), or a staged digital wallet operator (SDWO) uses cardholders’ payment credentials (i.e., account details) that they previously stored for future purchases.

Recognizing stored credential transactions distinctly allows for greater visibility into the transaction risk, enabling robust processing and resulting in differential treatment.

**How do merchants benefit from the Stored Credential framework?**

Identifying stored credential transactions specifically, allows for differentiated treatment through the authorization approval process. The results are:

- Greater visibility of transaction risk levels for issuers
- Results in higher authorization approval rates and completed sales
- Fewer customer complaints and improved cardholder experience
- Allows participation in Real Time Visa Account Updater Service3

The framework also allows participation in Real Time Visa Account Updater Service that enables real time updates as part of standard authorization process, eliminating the pre-authorization step currently required.

**What’s the impact on CyberSource Merchants?**

The Stored Credential construct is mandatory for all transactions where payment credentials are initially stored by the merchant and used for subsequent transactions. Compliance with the framework allows the real-time account updater service to provide updates as part of standard authorization transactions, eliminating the gap in time between current VAU and authorization transactions.

Merchants and their third-party agents, payment facilitators, or staged digital wallet operators that offer cardholders the opportunity to store their credentials on file must:

- Obtain cardholder consent for initial storage of credentials
Utilize appropriate data values (i.e., Stored Credential indicators as per the Stored Credential Transaction Framework) to identify initial storage and usage of stored payment credentials

Key Points

- Changes are mandated for all transactions where payment credentials are initially stored and used for subsequent transactions.
- No changes to current processing rules have been put into effect at Visa, but we expect them to be made sometime in 2018.
- Stored Credential transactions might be eligible for a differentiated treatment in future, though nothing announced as of today.
- Stored Credentials framework provides greater visibility of transaction risk levels leading to less likelihood of rejection.

What changes to CyberSource integration do I make to comply with the mandate?

All Stored Credential transactions, including the initial consumer initiated transaction when the credentials are stored on file and subsequent merchant initiated transactions using the stored credentials, must include the below data values defined by the framework to comply with the mandate:

**Consumer Initiated transaction indicator**: To identify a transaction as the initial consumer initiated transaction (CIT) wherein the merchant stores the payment credentials of the cardholder on its file, the API field ‘subsequent_auth_first’ must be included in the request.

**Merchant initiated transaction indicator**: To identify a transaction as MIT the API field “subsequent_auth” needs to be included in the transaction.

**Installment/Recurring transactions indicator**: There is no change in the way Installment or Recurring type of transactions are marked. They must continue to use API field ‘e_commerce_indicator’.

**Unscheduled card on file**: All transactions using card on file payment credentials must be marked using API field ‘subsequent_auth_stored_credentials’.

Additionally, while capturing the cardholder’s credentials for the first time for storing, whether PAN or payment token, merchants must:

- Obtain cardholder’s consent for storage of credentials and disclose the purpose.
- Submit a payment transaction, authorization or full financial transaction, if an amount is due or, if no amount is due, submit an account verification service transaction.
In case of a decline of the payment or account verification transaction, the credentials must not be stored or used for subsequent card on file transactions.

What’s the impact on CyberSource?

As this framework is rolled out and implemented by our acquirers and processors, CyberSource will be making updates to our connection interfaces to comply with the new specifications defined in support of Stored Credentials. Currently, in order to comply with the mandate, a number of our processor and acquiring partners are in the process of updating their system to meet the October 2017 mandate. CyberSource connections will be upgraded based on the mandate implementation date on the processor systems, with priority going to those connections that support Network Tokens.

Key Points

• Processors & Acquirers are updating their systems to support Stored Credential mandate
• CyberSource is updating all its connections to support Stored Credential mandate

What are Stored Credentials Use Cases?
**MIT**: In the event when payment credentials are not provided by the cardholder, instead are fetched from the merchant’s system all MITs are considered Stored credential transactions and must include the identifiers defined by the Stored Credential mandate.

**Credential on File (CoF)**: A card-absent transaction initiated by the cardholder where the cardholder does not need to enter their card details as the merchant uses the payment credential previously stored by the cardholder to perform the transaction. Examples include the Uber mobile app to hail a ride, ordering food from a food delivery service like DoorDash, and even buying on Amazon using your stored credentials from a prior order. These are just some of the payment experiences that CoF can provide consumer benefits.

**What are the resources available to help merchants with this Stored Credential framework? How can I learn more?**

CyberSource technical guide provides details on new API’s introduced by CyberSource to enable merchants comply with the mandate: [http://apps.cybersource.com/library/documentation/dev_guides/CC_Svcs_SCMP_API/Credit_Cards_SCMP_API.pdf](http://apps.cybersource.com/library/documentation/dev_guides/CC_Svcs_SCMP_API/Credit_Cards_SCMP_API.pdf)

The resource center at [https://www.cybersource.com/mitsc_mandate/](https://www.cybersource.com/mitsc_mandate/) is the best place to start. Merchant Support is also available to help guide merchants through this change.