Improving Authorization Management for Transactions with Stored Credentials

For merchants, acquirers, payment facilitators, and staged digital wallet operators that process stored credential transactions, and for all issuers.

The information provided in this guide allows all stakeholders to comply with the mandatory requirements and take advantage of the benefits of the Stored Credential Transaction framework.

Table of Contents

Introduction

Visa announced requirements for its Stored Credential Transaction framework, including mandates to identify initial storage and subsequent use of payment credentials.

What is a Stored Credential?

A stored credential is information (including, but not limited 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.

Chargeback Rules

Note:
There is no impact to chargeback rules as a result of these stored credential updates.

As the payment system has evolved, instances in which a transaction is initiated with a stored credential based on a cardholder's consent for future use have increased to significant levels.

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.

Visa has defined authorization data values to help identify initial storage and usage of stored payment credentials to enable differentiated processing.

Visa is enhancing its rules and processing specifications to address a comprehensive list of scenarios where payment credentials are stored with the merchant[1].

Note: Compliance with the Stored Credential Transaction framework is required to participate in Real Time Visa Account Updater[2]. This service enables merchants to get updated card information as part of the authorization message in real time, instead of the existing offline batch process.

Benefits of Identifying Transactions as a Stored Credential

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 Service[3]

1 Merchant refers to a merchant or its agent, a payment facilitator, or a staged digital wallet operator.
2 Availability varies by region.
3 Real Time Visa Account Updater expands VAU into VisaNet and enables real-time updates as part of the standard purchase authorization process. It eliminates the pre-authorization step required by legacy VAU, thus eliminating the gap in time between current VAU and authorization transactions.

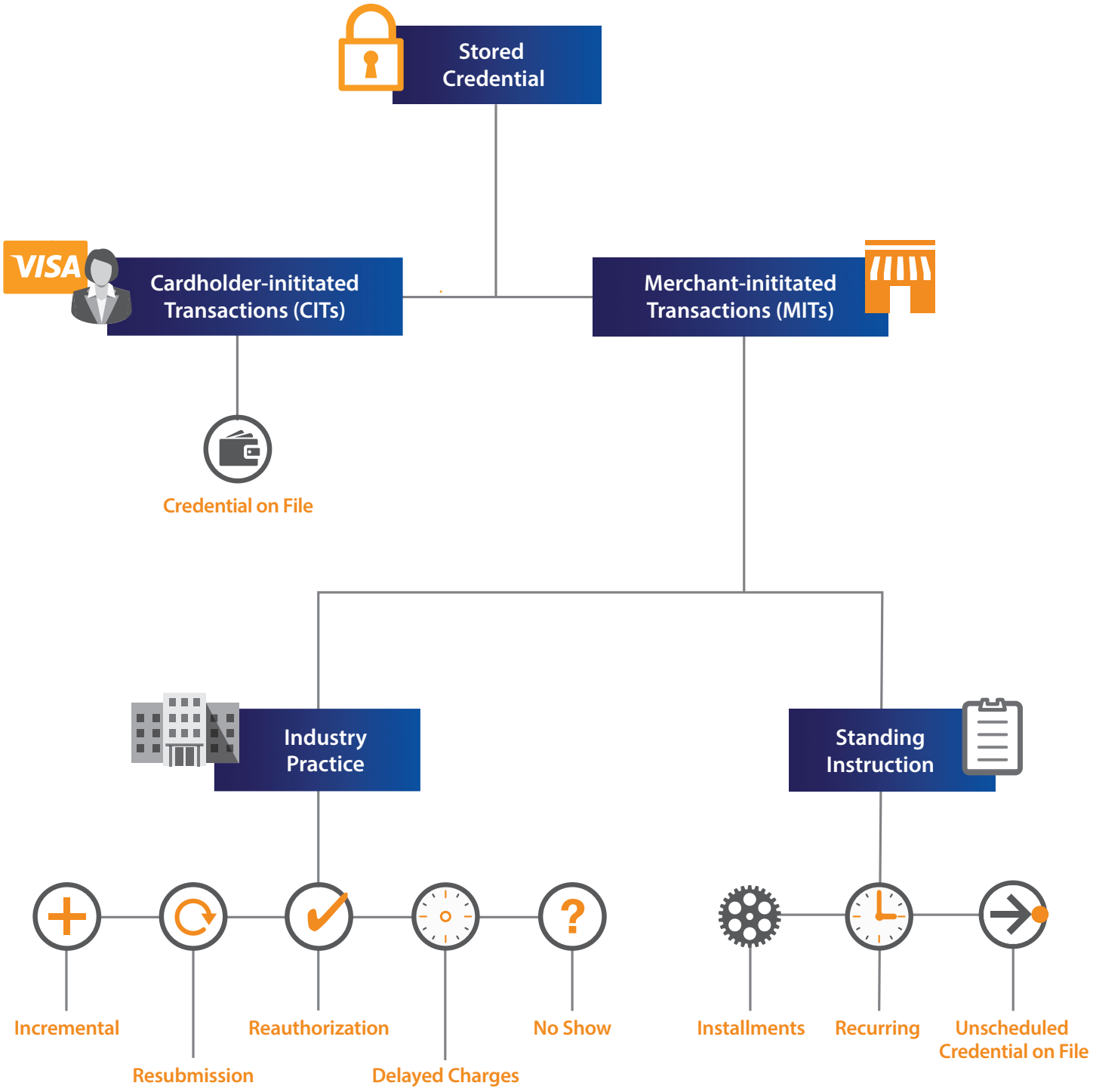
What is a Stored Credential?

A stored credential is information (including, but not limited to, an account number or payment token) that is stored by a merchant or its agent, PF, or SDWO to process future purchases for a cardholder.

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.

New Taxonomy for Stored Credential Transactions



Stored Credential Terminology

Cardholder-initiated Transaction (CIT): A cardholder-initiated transaction is any transaction where the cardholder is actively participating in the transaction. This can be either at a terminal in-store or through a checkout experience online, or with a stored credential.

Credential on File CIT: 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 a transaction using customer's merchant profile or staged digital wallets.

Merchant-initiated Transaction (MIT): Merchants commonly initiate MITs 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.

Industry-Specific Business Practice MITs: MITs defined under this category are performed to fulfill a business practice as a follow-up to an original cardholder-merchant interaction that could not be completed with one single transaction. Not every industry practice merchant-initiated transaction is performed with a stored credential. When the merchant or its agent, a payment facilitator, or a staged digital wallet operator stores the credential for a single transaction or a single purchase, it is not considered as a stored credential transaction. The following transaction types are industry-specific transactions:

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 represent 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.

Stored Credential Terminology (continued)

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.

Standing-Instruction MITs: MITs defined under this category are performed to address pre-agreed standing instructions from the cardholder for the provision of goods or services. The following transaction types are standing instructions transactions:

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.

Summary of Requirements

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**

Business Requirements for Processing Stored Credential Transactions

Effective October 2016:

Visa updated and expanded existing rules related to requirements to cover all transactions under the new stored credential transaction category.

Effective October 2017:

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

- Disclose to cardholders how those credentials will be used.
- Obtain cardholders' consent to store the credentials.
- Notify cardholders when any changes are made to the terms of use.
- Inform the issuer via a transaction that payment credentials are now stored on file.
- Identify transactions with appropriate indicators when using stored credentials.

Please refer to the October 2016 and April 2017 *Visa Global Technical Letter and Implementation Guide* and *Visa Rules* for complete details and to ensure compliance by the effective dates.

Disclosure requirements and indicator usage as per the Stored Credential Transaction Framework:

Effective with the 14 October 2017 VisaNet Business Enhancements Release, compliance with both disclosure requirements and usage of correct indicators is mandatory.

Global Stored Credential Transaction Framework Mandates

Effective October 2017 Globally

In an effort to align requirements globally, **effective 14 October 2017**, Visa requires:

- **When capturing a stored credential for the first time,** a merchant or its agent, a PF, or SDWO must:
  - Follow all cardholder disclosure and consent requirements specified in the Visa Rules.
  - Submit a payment transaction (authorization/full financial) to Visa if an amount is due at the time credentials are stored. If no amount is due at the time credentials are stored, the merchant or its agent, a PF, or an SDWO must submit an Account Verification authorization.

    Note: This requirement already exists for recurring and installment transactions in the Europe region.
  - Identify in the payment transaction or Account Verification authorization that the credential is being stored:
    - If the credential is being stored for cardholder-initiated, stored credential transactions or for Unscheduled Credential-on-File (UCOF) transactions, the merchant or its agent, a PF, or an SDWO must submit the value **"C"** in the **POS Environment** field.
    - If the payment credential is being stored for a recurring or installment relationship, the merchant or its agent, a PF, or an SDWO must submit the transaction with the existing value of **"R"** or **"I,"** respectively in the **POS Environment** field.

  Note: If either the first payment or the Account Verification authorization is declined, the credential cannot be considered a stored credential, and the merchant must not use the credential for any subsequent transactions.
- **When initiating a transaction using a stored credential**, the merchant or its agent, a PF, or an SDWO must submit the payment transaction with a value **"10"** in the **POS Entry Mode Code** field. Value "10" indicates the credential presented is a stored credential.

This applies to **card-absent transactions** using stored credentials, including transactions that are:

- Performed with primary account numbers (PANs) or payment tokens.
- Initiated by a cardholder for purchases of goods or services with payment credentials already stored by the merchant or its agent, a PF, or an SDWO.
- Initiated by the merchant without active participation of the cardholder:
  - Based on standing instructions with the cardholder (i.e., recurring, installment and UCOF transactions). Standing instruction transactions for recurring, installment or UCOF transactions must be submitted with an "R," "I," or "C," respectively, in the POS Environment field.

    OR
  - For industry-specific business practice MITs such as incremental payments, no shows, delayed charges, reauthorization, or resubmission where the credentials were previously stored for future purchases (and not to complete that specific transaction only).

Note: Subsequent merchant-initiated recurring, installment, or UCOF standing-instruction transactions must always be submitted with a POS Entry Mode Code of "10." Standing-instruction transactions are only permitted when credentials are stored on file.

4 Merchant refers to a merchant or its agent, a payment facilitator, or a staged digital wallet operator.

Face-to-face Environment

The following two tables highlight the correct POS Entry Mode Codes and POS Environment field values for initial and subsequent cardholder-initiated transactions (CITs) and merchant-initiated transactions (MITs):

First Transaction Setting		Storage of Credential for Future Transactions	Does Storage of Credential Mandate Apply?	First Transaction		Subsequent Transactions (Card-Absent Environment)				
						CIT		MIT		
									POS Environment	
Environment	Form Factor			POS Entry Mode	POS Environment	POS Entry Mode	POS Environment	POS Entry Mode (Industry Practice or Standing Instruction)	Industry Practice	Standing Instruction
Face-to-face	Payment card or pass-through digital wallet at merchant POS terminal	Merchant or its agent or PF	Yes	07, 90, 91, 01	C, R, or I (as appropriate)	10	Field not present	10	Field not present	C if UCOF, R if recurring, or I if installment
		Not stored by merchant or its agent or PF	No		Field not present	No subsequent transaction with a stored credential		01 (any valid value for incremental except 10)	Field not present	N/A (transaction not permitted)

Card-absent Environment

The following two tables highlight the correct POS Entry Mode Codes for initial and subsequent cardholder-initiated transactions (CITs) and merchant-initiated transactions (MITs):

First Transaction Setting		Storage of Credential for Future Transactions	Does Storage of Credential Mandate Apply?	First Transaction		Subsequent Transactions (Card-Absent Environment)				
						CIT		MIT		
									POS Environment	
Environment	Form Factor			POS Entry Mode	POS Environment	POS Entry Mode	POS Environment	POS Entry Mode (Industry Practice or Standing Instruction)	Industry Practice	Standing Instruction
Card-absent	Merchant profile or pass-through digital wallet (online or mobile)	Merchant or its agent or PF	Yes	01	C, R, or I (as appropriate)	10	Field not present	10	Field not present	C if UCOF, R if recurring, or I if installment
		Not stored by merchant or its agent or PF	No		Field not present	01 (subsequent transaction with a stored credential not permitted)	Field not present	01 (any valid value for incremental except 10)	Field not present	N/A (transaction not permitted)
	SDWO	SDWO	Yes	01	C, R, or I (as appropriate)	10	Field not present	10	Field not present	C if UCOF, R if recurring, or I if installment

Use and Definition of Value "C" in the POS Environment Field

"C"

The value "C" in POS Environment field indicates one of the following:

- The merchant or its agent, a PF, or an SDWO is storing the payment credential for the first time for subsequent cardholder-initiated transactions.
- The merchant or its agent, a PF, or an SDWO is storing the payment credential for the first time for subsequent UCOF transactions.
- The merchant or its agent, a PF, or an SDWO is submitting an UCOF transaction, which is initiated based on standing instructions with the cardholder. UCOF transactions are triggered by events that do not occur at a scheduled interval—for example, a cardholder sets up a reload of their account with the merchant based on usage thresholds, which does not occur at regular intervals[5].

Note: Use value "10" for the POS Entry Mode Code and value "C" for the POS Environment field in the same transaction only if it is an UCOF transaction. Cardholder-initiated, stored credential transactions must only use the POS Entry Mode Code value "10" and no POS Environment field.

Note: For Visa card transactions that are not processed by VisaNet, processors may use other values and/or fields for the purposes listed above, as long as specific indicators are used.

5 When a standing instruction transaction is initiated at regular intervals, the recurring transaction indicator "R" should be used.

Consent Agreement Provisions

Disclosure to cardholder and cardholder consent[6]

Note:
Retroactive identification and cardholder consent and disclosure agreement are not required for credentials stored prior to 14 October 2017. However, effective 14 October 2017, a merchant or its agent, a PF, or an SDWO must submit all stored credential transactions with a value of "10" in the POS Entry Mode Code field, including transactions for credentials stored prior to this date.

Prior to storing credentials for future use, the merchant or its agent, the payment facilitator, or the staged digital wallet operator must establish an agreement with the cardholder.

Basic Requirements:

- Truncated version of the stored credentials (i.e., last four digits of PAN)
- How the cardholder will be notified of any changes to the consent agreement
- The expiration date of the consent agreement, if applicable
- How the stored credential will be used

Additional Requirements:

If the cardholder is providing consent to the merchant or its agent, a payment facilitator, or a staged digital wallet operator to initiate transactions using stored credentials.

- Cancellation and refund policies
- Location of merchant
- Transaction amount or how it will be calculated
- Convenience fee or surcharge (if permitted and applicable)
- The frequency (recurring) or event (unscheduled) that will prompt the transaction
- For installment payments, the total purchase price and terms of future payments, including the dates, amounts, and currency

Handling and storage requirements

Basic Requirements:

- Notify the cardholder in the event of a change to the agreement
- Retain the agreement for duration of the consent; provide it to the issuer upon request
- Where required by applicable laws or regulations, provide to the cardholder a record of the consent

Do not complete a transaction:

- Beyond the duration expressly agreed by the cardholder, or
- If the cardholder requests that the merchant or its agent, a payment facilitator, or a staged digital wallet operator change the payment method, or
- If the cardholder cancels according to the agreed cancellation policy, or
- If the merchant or its agent, a payment facilitator, or a staged digital wallet operator receives a decline response

Other requirements

Authentication:

For a transaction using a stored credential initiated by the cardholder, the merchant or its agent must validate the cardholder's identity before processing. Local regulations and laws must be followed as appropriate.

Receipts:

Receipts must be provided for installments; if the cardholder cancels the installment within the terms of the cancellation policy, within three business days the merchant or its agent, a payment facilitator, or a staged digital wallet operator must provide cancellation or refund confirmation in writing and credit transaction receipt for the amount specified in the cancellation policy.

6 Not applicable to no show, delayed charge, incremental authorization, resubmission, reauthorization.

Additional Information

Existing stored credentials	Retroactive identification and cardholder consent and disclosure agreement are not required for credentials stored prior to 14 October 2017. However, **effective 14 October 2017**, a merchant or its agent, a PF or an SDWO must submit all stored credential transactions with a value of "10" in the POS Entry Mode Code field, including transactions for credentials stored prior to this date.
Stored credential with third parties	Credentials can be on file with the merchant, its agent, a payment facilitator, or a staged digital wallet operator. If the merchant is unsure whether payment credentials were in storage, the stored credential indicator should not be used. For example, this would apply when a hotel booking has been made through an online travel agent.
"Guest" checkout with additional charges (industry-specific practices)	If guest[7] checkout is utilized but payment credentials are provided/stored to cover additional related charges associated with solely that transaction—i.e., split shipments, delayed hotel charges—Stored Credential indicators should not be used.
Declined initial transaction	If the initial transaction (in which storage of credentials is communicated) is declined for any reason, the merchant should not consider the credential to be on file for the purpose of the Stored Credential indicator.

When is the credential considered stored?	Once the merchant has:
	• Followed all disclosure requirements; and
	• Used the appropriate indicator in the authorization message to:
	  • Indicate that the credential is being stored, and
	  • Request and receive approval on the authorization for the initial transaction
	Note: When a merchant does not take any payment at the time of storing the credential on file, the merchant must submit an Account Verification transaction.

When is the credential NOT considered stored?	A credential is not considered stored when the merchant or its agent stores the credential to complete a single transaction or a single purchase (including multiple authorizations related to the 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. Also, 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.

7 A cardholder is considered checking out as a "guest" when he or she completes an online transaction without registering or logging in.

Europe Additional Requirements

Effective October 2017

Additional acquirer/merchant requirements for stored credentials used for the purpose of merchant-initiated transactions in Europe.

Merchant-Initiated Transactions in Europe	Provide notification for recurring transactions (seven business days) and for Unscheduled COF transactions (two business days) before any of the following: • End of trial period • More than six months have elapsed since the previous transaction in the series • Any change to the agreement including date, amount, or how it is calculated
Card Verification Value Requirements	An issuer must not decline a transaction based solely on a missing CVV2, if the authorization request is for the subsequent transaction after the credential is stored. This rule previously applied only to recurring transactions and is now applicable to: • Recurring • Installment • Unscheduled COF (UCOF) • Transactions initiated by the cardholder using a stored credential

For More Information

AP, Canada, CEMEA, LAC, U.S.:
Contact your Visa representative. Merchants and third party agents should contact their issuer or acquirer.

Europe:
Contact Europe Customer Support on your country-specific number, or email CustomerSupport@visa.com.