The Payment Card Networks (PCNs) are making changes to rules governing transaction processing by introducing instructions as to how Cardholder payment information (credentials) must be obtained, stored and processed. The changes are being implemented by PCNs to improve the Cardholder experience by increasing authorization rates and reducing the number of Cardholder complaints and disputes. These requirements for storing Cardholder payment information will be effective as of **September 1, 2019.**

Any business that offers Cardholders the opportunity to store their payment information on file to process transactions must:

- Disclose to Cardholders how their credentials will be used.
- Obtain and retain Cardholders' consent to store their credentials.
- Notify Cardholders when any changes are made to the terms of use.
- Ensure transactions contain the necessary payment details when storing or using cards on file (payment information). Refer to the Additional Information section below for more details.

The following includes answers to frequently asked questions and additional information that will be helpful to understand the PCN transaction processing requirements related to obtaining, storing and processing Cardholder payment information.

What is required to obtain Cardholder consent to process future credential on file transactions?
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. The basic elements of the Agreement should include:

- Truncated version of the stored credentials (e.g. last four digits of Primary Account Number (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.

What is required after the consent is obtained?
Once the consent has been obtained, a Merchant or its Agent, the payment facilitator or the staged digital wallet operator must:

- 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.

Are these new requirements mandatory to implement?
If you are a Merchant who stores credentials for transaction processing you will be required to comply with the new requirements. Furthermore, if you are using any solution providers (e.g. website or shopping cart provider) for processing your ecommerce payment transactions, please contact them to review any changes that may be required to the integration.

For technical information about changes you and/or your solution provider(s) may need to make, please review our online documentation.

What does a Merchant need to do with existing credentials stored on file?
For any payment information saved on file prior to September 1, 2019, TDMS recommends obtaining and storing the Cardholder consent as well as the Agreement with the Cardholder.

ADDITIONAL INFORMATION

What is a stored credential?
A stored credential is information that is stored by a Merchant to process future transactions for a Cardholder. Stored credentials (payment information) are obtained through an interaction with a Cardholder and may be used for an initial transaction or subsequent future transactions based on an Agreement with a Cardholder.

What is a stored credential transaction?
A transaction using Cardholder's stored payment credentials. Stored credential transactions must contain all the necessary transaction details as per the Payment Card Network requirements.

Authorized Use of Stored Credentials:
For your reference, the following definitions explain the various types of authorized stored credential transactions.

Cardholder Initiated Transaction (CIT):
This is a transaction that is completed by the Cardholder. Customer initiated transactions include both initial and subsequent transactions.

> **Initial CIT:**
> This is the first transaction completed by the Cardholder; during the transaction the Merchant obtains Cardholder agreement to store their credentials on file for future use (e.g. online shopping, first visit).
>
> **Subsequent CIT:**
> A transaction initiated by the Cardholder where the Cardholder does not need to enter their payment card details because the Merchant uses the payment credentials previously stored during the initial CIT (e.g. online shopping, subsequent visit).

Merchant Initiated Transaction (MIT):
This is a transaction that is completed by the Merchant using a Cardholder's stored credentials without the active participation of the Cardholder. For these transactions, the Cardholder consent has been previously provided and stored. Below are two examples of different types of Merchant initiated transactions:

> **Recurring Payment:**
> A recurring payment is a transaction in a series of transactions that occurs at fixed, regular intervals. It uses a stored credential based on an Agreement between the Merchant and Cardholder to process recurring transactions (e.g. gym membership, book of the month club).
>
> **Unscheduled Payment (also known as an Unscheduled Credential on File Transaction):**
> This transaction is completed using a stored credential that does **not** occur on a scheduled or regularly occurring transaction date (e.g. an Account auto top up transaction like Coffee Cards and Transit passes).

Important Reminder: All CITs and MITs must have all the proper indicators included to specify the type of transaction being completed.

Unauthorized Use of Stored Credentials:
The following scenarios are examples of when a Merchant is **not** permitted to complete stored credential transactions:

- The duration is beyond the expressly agreed timeframe by the Cardholder;
- The Cardholder requests that the Merchant or its Agent, a payment facilitator or a staged digital wallet operator change the payment method;
- The Cardholder cancels according to the agreed cancellation policy as outlined in the Agreement;
- The Merchant or its Agent, a payment facilitator or a staged digital wallet operator receives a decline response to a processed transaction.