LLOYDS BANK | CARDNET

STORED CREDENTIAL & CREDENTIAL-ON-FILE GUIDE

December 2017

VISA RULES

SUMMARY OF A STORED CREDENTIAL

A stored credential is information which may include an account number or payment token that is stored by a Merchant. Stored credentials are eligible for any purchase.

A stored credential could be a Cardholder Initiated Transaction or a Merchant Initiated Transaction:

Cardholder Initiated Transactions(CIT)	Merchant Initiated Transactions (MIT)
Transaction where the cardholder actively participates in the transaction	Any transaction that relates to a previous cardholder-initiated transaction but is conducted without the active participation of the cardholder. To: • Perform a transaction as a follow-up to a CIT (Industry practices) • Perform a pre-agreed standing instruction from the cardholder for the provision of goods or services
Standard in-store or online checkout transaction, or with a stored payment credential that the cardholder has previously consented to store with the merchant.	
Cardholder authentication always available e.g. signature, Verified by Visa, wallet sign-in (i.e. Visa Checkout), other form of ID	
May be followed by subsequent transactions initiated by the Merchant when a Consumer-Merchant interaction is established	Cardholder authentication is never performed
Determines how subsequent transactions initiated by Merchant should occur, if any	When MIT framework is used, must have proof of a preceding online authorised message

A merchant may use stored credentials for the following type of transactions:

- **Unscheduled Credential on file transaction (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.

- **Instalment transaction –** 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 of time for a single purchase of goods or services

- **Recurring transaction -** 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.

STORED CREDENTIAL REQUIREMENTS*

In effect from October 2017 Merchants & Acquirers must:

- Obtain Cardholder consent for initial storage of payment credentials
- Send data values (i.e. Stored Credential indicators) to identify initial storage and usage of stored payment credentials

When capturing a stored credential for the first time a merchant/acquirer must:

1. **Follow all cardholder disclosure & consent requirements–** This is listed below in the Stored Credential Rules section
2. **Request authorisation at time of storing credentials**
   - ✓ Where a Merchant does not take any payment at the time of storing the Credential the Merchant must submit an Account Verification Service Transaction
   - ✓ If either the first payment or the Account Verification Service Transaction are declined, the payment credential cannot be considered a Stored Credential and the merchant/acquirer must not store/ use the credential for any subsequent transactions.
   - ✓ Identify in the authorisation message that the credential is being stored using the appropriate indicator in the POS environment Field (Field 126.13)
     - ❖ "C" for future customer initiated credential on file transactions or for future UCOF
     - ❖ "R" if for future Recurring
     - ❖ "I" if for future Instalment
3. **When initiating a subsequent transaction using a Stored Credential, a merchant/acquirer must**
   - ✓ Use the POS Entry Mode code of 10 that shows the transaction is being performed with a Stored Credential in both the Authorisation Request and in the Clearing Record
     - ❖ "R" present if Recurring and "I" present if Instalment
     - ❖ "C" present only if UCOF –not if **cardholder initiated transaction**

STORED CREDENTIAL RULES

A merchant, payment facilitator or digital wallet operator that stores a Stored Credential and or processes Transactions using a stored credential must comply with the following rules which came in to effect 14 October 2017:

1. Must establish an agreement with the cardholder which contains all of the following:
   - ✓ A shortened version of the stored credential. E.g. last 4 digits of the account number
   - ✓ How the cardholder will be notified of any changes to the agreement
   - ✓ How the stored credential will be used
   - ✓ Expiration of the agreement, if applicable

2. Before processing an instalment, recurring transaction must establish an agreement with cardholder which contains all of the following:
   - ✓ Cancelation and refund policies
   - ✓ The location of the merchant outlet
   - ✓ Transaction amount (Inc. taxes and charges) or a description of how the amount is determined
   - ✓ Transaction currency
   - ✓ Where surcharging is permitted, acknowledgement of any surcharge assessed and the associated disclosures
   - ✓ For instalment transactions –Total purchase price & terms of future payments, dates, amount & currency
   - ✓ For recurring transactions the fixed dates/intervals on which the transactions will be processed
   - ✓ For unscheduled credential on file transactions, the event that will prompt the transaction. E.g. the cardholders balance falls below a certain amount

3. Must retain the cardholders agreement for the duration of the agreement and provide to the issuer upon request

4. The amount for an instalment transaction may include interest charges (except in the U.S region)

5. For a recurring transaction or an unscheduled credential on file, the amount must not include finance charges

6. Transaction processing:
   - ✓ Zero Floor Limit (authorisation required) for each transaction. The amount authorised must be no more than the amount of the individual transaction
   - ✓ For a transaction initiated by the cardholder, the merchant must validate the cardholders identity e.g. with login & password before processing each transaction

7. Transaction processing for an instalment transaction, all of the following apply:
   - ✓ If an authorisation request for a subsequent payment is declined, the merchant must notify the cardholder, allowing at least 7 days to pay by other means
   - ✓ A merchant must not process an initial instalment transaction until the merchandise or services have been provided to the cardholder and must not process individual instalment transactions at intervals less than either:
     - ❖ 7 Calendar days
     - ❖ In the US region, the monthly anniversary of the shipment date
   - ✓ Visa assumes no liability for an Instalment transaction processed more than 30 calendar days from the authorisation date

8. Cancellation procedure, the merchant must:
   - ✓ Provide a simple cancellation procedure, or if the cardholder's order was initially accepted online, an online cancellation procedure
   - ✓ Not complete a transaction:
     - ❖ Beyond the duration expressly agreed by the cardholder
     - ❖ If the cardholder requests that the merchant change the payment method
     - ❖ If the cardholder cancels according to the agreed cancellation policy
     - ❖ If it receives a declined response
   - ✓ For an instalment transaction, if the cardholder cancels within the terms of the cancellation policy, the merchant must provide the cardholder both of the following within 3 business days:
     - ❖ Cancellation or refund confirmation in writing
     - ❖ Credit transaction receipt for the amount specified in the cancellation policy.
9. The merchant must refund the full amount paid if the merchant has not adhered to the terms of the sales of service

These requirements do not apply when the merchant uses the stored credential for a single transaction or a single purchase for:

- No show transaction
- Transaction involving an amended amount or delayed charge
- Incremental Authorisation
- Merchant is allowed to submit a new authorisation request for the same transaction
- Declined response and is resubmitted for Authorisation

Visa has granted Lloyds Bank Cardnet more time to comply with these new requirements. Our merchants have a waiver for these rules until 30 April 2018. In addition, our merchants have until 31 October 2018 to provide the transaction indicators in the authorisation message.

MASTERCARD RULES

CREDENTIAL-ON-FILE REQUIREMENTS & CREDENTIAL-ON-FILE INDICATOR*

A credential-on-file transaction is a transaction in which a cardholder explicitly authorised a merchant or payment facilitator's sub merchant to store the cardholder's Mastercard or Maestro account (primary account number [PAN] and expiration date, or tokenised PAN and expiration date) and subsequently the cardholder authorises that same merchant to bill the cardholder's stored Mastercard or Maestro account.

A credential-on-file transaction can be individual cardholder-initiated transactions (such as an e-commerce transaction, mail order transaction, or phone order transaction) or, as a result of an agreement with the cardholder, merchant-initiated (such as a recurring payment or instalment payments).

The Acquirer should ensure that the Merchant retains the Cardholder's written agreement to the terms of a Credential-on-file Transaction arrangement.

Effective 12 June 2018, a Credential-on-file indicator is required for

- ✓ Authorisation of a Credential-on-file Transaction which is a value of 10 (Credential on File) in DE 22 (Point-of-Service Entry Mode), subfield 1 (POS Terminal PAN Entry.)

- ✓ Clearing transactions, of a Credential-on-file Transaction which is a value of 7 (Credential on File) in DE 22 (Point-of-Service Entry Mode), subfield 7 (Card Data Input Mode).

The credential-on-file indicator

- Allows a merchant to communicate a pre-existing relationship with a cardholder to the issuer, using an identifier that is common across the industry. A repeat customer should have a lower risk profile than a first time or "guest" check-out customer.
- Increase transaction transparency for issuers to facilitate risk management, fraud management, and authorisations
- Increase transaction transparency for issuers (such as the transaction is credential-on-file and recurring, the transaction is credential-on-file and e-commerce, or the transaction is credential-on-file and telephone order)

An acquirer must ensure that the acquirer and each of its Third Party Processors (TPPs) technically supports the passing of the credential-on-file indicator in authorisation and clearing messages for each transaction identified by a merchant as a credential-on-file transaction.

Examples of Credential-on-File Transactions

These examples do not represent the only transactions that should use the credential-on-file indicator. There may be other scenarios in which the credential-on-file indicator should be used.

- **E-Commerce:** Any e-commerce transaction made from a merchant website where the cardholder has saved a credential-on-file with the merchant for future cardholder initiated bill payments or purchases including retail stores, airlines, hotels, and online travel agencies. Any e-commerce transaction made from a merchant mobile app where the cardholder has saved a credential-on-file with the merchant for future orders including categories such as restaurant meal delivery, ride hailing, music downloads, app stores, and in-app purchases. With the rise of "order online, pick-up in store," the credential-on-file indicator should be used if the cardholder pays online with a saved credential-on-file. The new indicator should not be used when a payment is made in-store and credentials were not saved by the merchant.

- **Recurring Payments** - All recurring payments are considered credential-on-file transactions.

- **Instalment Payments** - All instalment payments are considered credential-on-file transactions.

- **Mail Order/Telephone Order (MO/TO)-** Any mail order or phone order transaction that occurs when the cardholder has saved a credential-on-file with the merchant and authorises the merchant to use the credential-on-file for the transaction should have the credential-on-file indicator including restaurant orders for delivery, pharmacy prescription mail/phone orders, and cardholder initiated bill payments.

- **Brick and Mortar**: While most credential-on-file transactions will be from card-not-present transactions, the indicator can be used in cardholder-present transactions where the cardholder has saved a credential-on-file

with the merchant and authorises the merchant to use a credential-on-file for a transaction. For example, a pharmacy that receives a walk-in customer for a prescription and the customer authorises the pharmacy to use the credential on-file to complete the transaction.

- **Account Status Inquiry Messages**: The presence of the new credential-on-file value within DE 22 (POS Entry Mode) should also be used within Account Status Inquiry (ASI) messages to indicate the card was already on file prior to submitting the ASI request. The absence of the credential-on-file value within a Purchase ASI or Recurring ASI message should indicate a one-time request to validate card status, or a request to validate prior to saving as credential-on-file for future purchases or recurring payments.

***Please ensure that any of your back office systems and integrated 3rd parties can accommodate these mandatory changes when authorising a credential on file transaction. Should you wish to discuss these changes in more detail please contact us on 0845 835 5723 and we'll be happy to help. Lines are open 9am to 5pm Monday to Friday.**