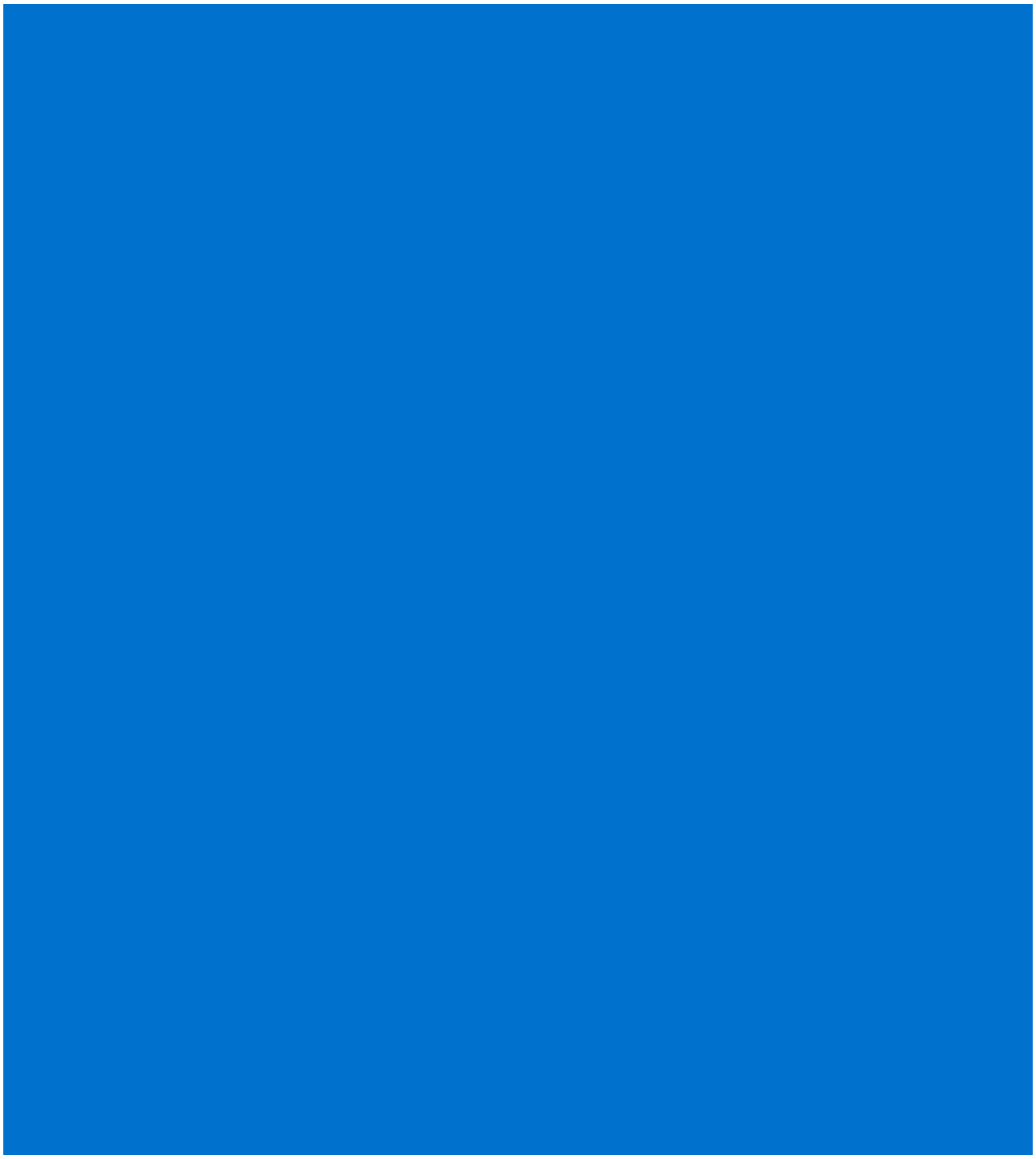
globalpayments

Stored Credential Guide

Merchant Operating Instructions Addendum



Contents

Introduction

As the payment system has evolved, with the growth in digital commerce and emergence of new business models, 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. Correctly identifying these transactions should result in higher authorisation approval rates and completed sales, and fewer customer complaints and an improved cardholder experience.

Added to this, the Payment Services Directive 2 has mandated that from **14th September 2019** all payments will have to be validated using Strong Customer Authentication (SCA). From that date, card issuers are obliged to seek SCA or decline transactions that aren't fully authenticated that should be. It's now more critical than ever that Stored Credential Transactions are flagged correctly or the card issuer may choose to challenge the transaction and request SCA. If the cardholder can't be contacted or provide SCA, the transaction won't go ahead.

For more details on SCA, how it works and what's required, see our *PSD2 and Strong Customer Authentication Technical Implementation Guide*, which is on our website at www.globalpaymentsinc.com/en-gb. You'll find this within our Customer Centre, under the option for Strong Customer Authentication.

What's a Stored Credential?

A stored credential is information, including but not limited to, a card number or payment token, that's stored by a merchant or a third party on their behalf to process future purchases for the cardholder.

Obtaining cardholder details isn't considered a stored credential when the merchant or a third party on their behalf, stores the details to complete a single transaction or a single purchase, including multiple authorisations related to that particular transaction. For example, when a cardholder provides their card details to a hotel to cover charges related to a specific reservation only. However, when a cardholder provides their card details to a hotel to cover future reservations and charges as part of the cardholder's membership profile it's considered to be a stored credential.

About this Document

This document is provided for guidance to merchants that use stored credentials. This document is an Addendum to the *Merchant Operating Instructions*.

Note: Except as specifically modified herein, all instructions provide in the *Merchant Operating Instructions* will remain unchanged and in full force and effect. In the event of any inconsistencies between the instructions in this Addendum and those in the *Merchant Operating Instructions*, the instructions herein shall prevail.

Types of Stored Credentials

All Stored Credential Transactions fall into one of two categories depending on whether the transaction is actively initiated by the cardholder (a Cardholder Initiated Transaction) or not (a Merchant Initiated Transaction). This section provides a full explanation and details the types of transactions that fit into these catefories. A diagram of the transaction types can also be found on page 4.

Cardholder Initiated Credential on File Transactions

A Cardholder Initiated Transaction (CIT) is any transaction where the cardholder is actively participating in the transaction. This can be either at a card terminal in a store or through a checkout online. In the Credential on File CIT scenario, the cardholder isn't present but initiates a transaction where they don't need to enter their card details as the merchant uses the card details previously stored by the cardholder to perform the transaction. For example, the cardholder inputs their card details for storage on a merchant website and then uses them to perform subsequent transactions at undefined periods.

To clarify, a payment made through an online app to purchase goods or services at the cardholder's request, for example, buying a train ticket, only falls within the Visa Stored Credential Transaction Framework if the card details are stored on the app for the cardholder to reuse. If the cardholder enters their card details every time they make a purchase, the Credential on File requirements don't apply.

All Cardholder Initiated Transactions, whether made with stored credentials or not are subject to SCA. In practice, that means that the cardholder must be authenticated using 3D Secure unless an explicit exemption is requested. Customer Initiated Transactions aren't automatically exempt from SCA. Please see our *PSD2 and Strong Customer Authentication Technical Implementation Guide*.

Merchant Initiated Credential on File Transactions

A Merchant Initiated Transaction (MIT) is commonly initiated by a merchant without any active participation from the cardholder. To do this, the cardholder would give the merchant consent to store their card details, making them Credential on File MITs. For example, a recurring payment for a magazine subscription.

To clarify, a payment made through an online app to purchase goods or services at the cardholder's request, for example, a one-click shopping experience, isn't a MIT as the cardholder actively participates in it.

Merchant Initiated Credential on File Transactions are further split into two categories and a described in more detail below:

- Standing Instructions
- Industry Practice

All MITs are out of scope for SCA provided that the transactions are correctly identified as Credential on File Transactions and have the correct exemption flagging on them. This will allow the card issuer to know that the customer isn't present and not request that the cardholder authenticates themselves. For SCA exemption purposes, a Recurring Transaction is classified as having a fixed amount. When the amount varies, then the MIT exemption flag is used. For full details of this flagging that should be applied and the rules for usage, please our *PSD2 and Strong Customer Authentication Technical Implementation Guide*.

Standing Instructions

MITs in this category are performed to fulfil pre-agreed standing instructions from the cardholder for the provision of goods or services. Standing Instructions are defined as the following types of transaction:

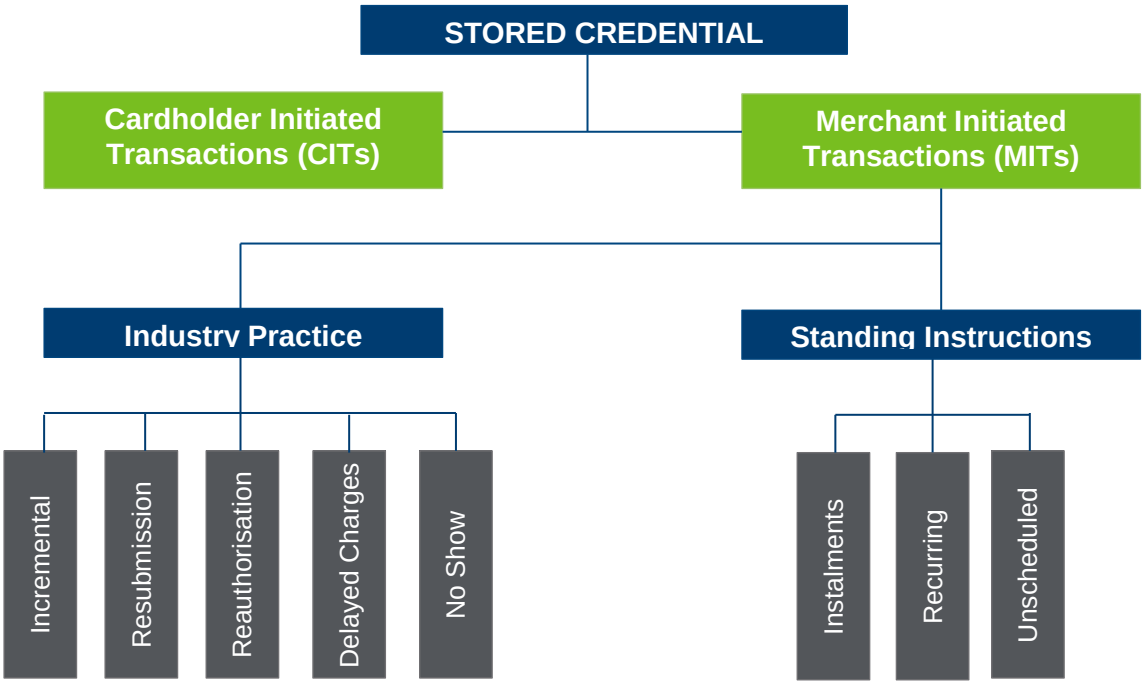
- **Recurring Transactions** – transactions that are processed on a regular fixed interval for a pre agreed or advised amount, where applicable. Recurring Transactions don't have a fixed duration and will continue to be processed until the cardholder cancels the agreement. For example, a magazine subscription. For SCA exemption purposes, a Standing Instructions is only classed as a Recurring Transaction if it's for the same amount every time.

- **Instalment Payments** – transactions that are processed on a regular fixed interval for a pre agreed amount for a single purchase of goods or services. Unlike Recurring Transactions, Instalment Payments do have a fixed duration and mustn't continue to be processed after the end of the agreed instalment period. For example, buying white goods on interest free credit over six monthly instalments.
- **Unscheduled Credential on File Transactions** – transactions that are for a fixed or variable amount that don't occur on a scheduled or regularly occurring transaction date, but when a pre-defined event happens. For example, an account automatic top up when it falls below a minimum amount.

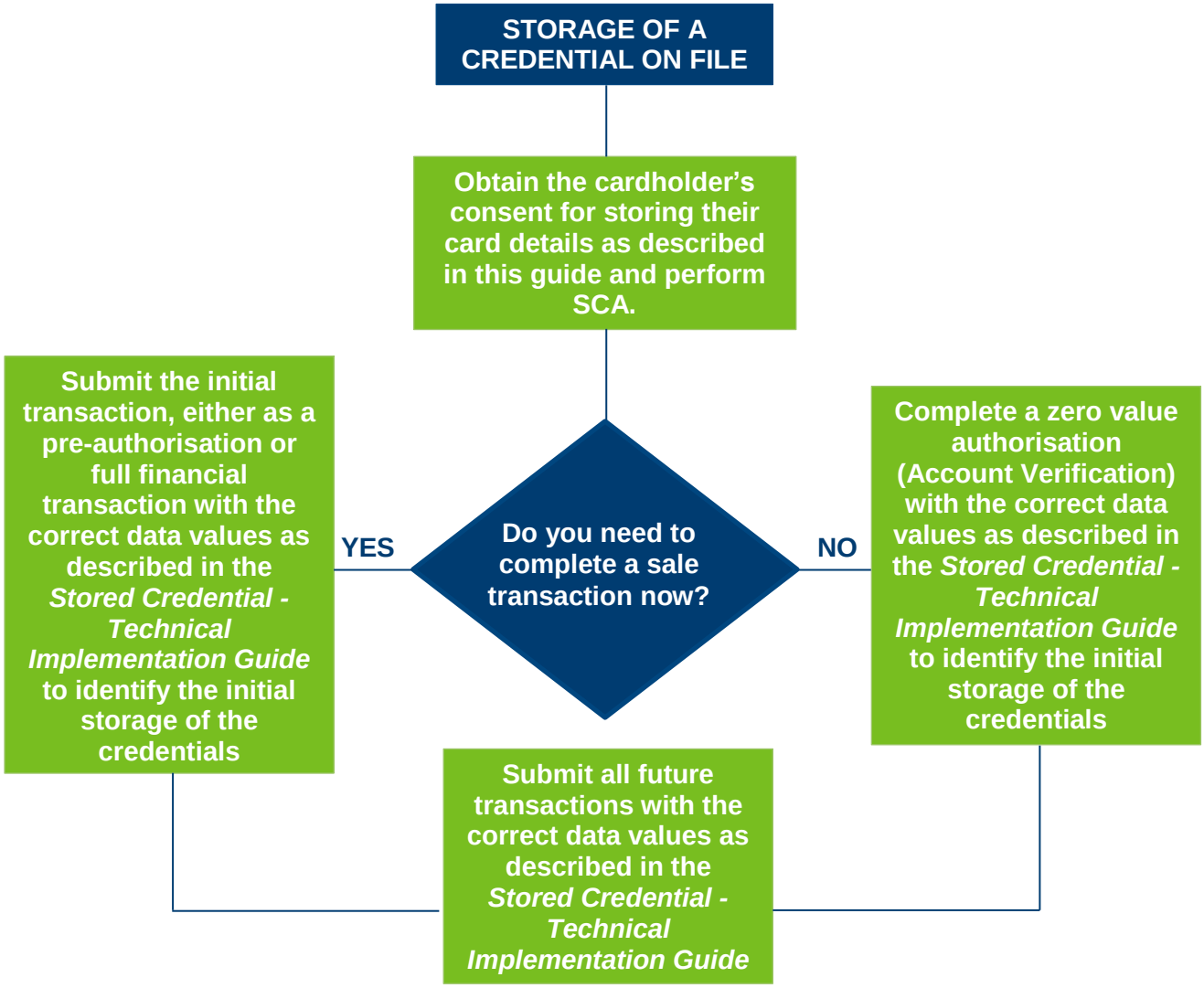
Industry Practice

These MITs reuse the cardholder's credentials as a follow-up to an original cardholder-merchant interaction that couldn't be completed in one single transaction. Industry Practice Transactions are defined as the following types of transaction:

- **Incremental Authorisations** – used to increase the total amount authorised if the original authorisation amount is insufficient. An Incremental Authorisation request may also be based on a revised estimate of what the cardholder may spend. A typical scenario where this type of transaction is used is when a cardholder checks into a hotel. For example, a guest may request a room only and then subsequently add a meal and drinks to their bill. Incremental authorisations don't replace the original authorisation, they're additional to previously authorised amounts. The sum of all linked estimated and incremental authorisations represent the total amount authorised for a given transaction. An Incremental Authorisation must be preceded by an estimated/initial authorisation. One or more Incremental Authorisations can be requested while the transaction hasn't been finalised (submitted for clearing). Incremental Authorisations mustn't be used once the original transaction has been submitted for clearing. In such a scenario, a new authorisation must be requested, with the appropriate reason code (for example, delayed charges, reauthorisations).
- **Resubmissions** – used when the original authorisation has been declined for insufficient funds.
- **Reauthorisations** – used when the validity period for a previous authorisation has expired. There are two common reauthorisation scenarios:
  - Split or delayed shipments by an online merchant. A split shipment occurs when not all the goods ordered are available for shipment at the time of purchase. If the fulfilment of the goods takes place after the authorisation validity limit set by Visa, online merchants perform a separate authorisation to ensure that cardholder funds are available.
  - Extended car rentals or lodging or cruise line stays. A reauthorisation is used for rentals, stays, or voyages that extend beyond the authorisation validity period set by Visa.
- **Delayed Charges** – used to process an additional charge after the original transaction has been completed. For example, in a hotel, the guest may not have disclosed that they'd used the mini bar. Or for car rentals, the hire company may charge for fuel if the car is returned without a full tank of petrol.
- **No Show** – used to charge a cardholder a penalty for not showing up for a reservation or a late cancellation in accordance with the merchant's cancellation policy. Typically used in the hotel sector to cover lost revenue from guests failing to turn up.



Summary of Requirements



If you, or a third party on your behalf, offer cardholders the opportunity to store their card details on file, you must:

- Obtain cardholder consent for the initial storage of their credentials, and
- Perform SCA for either the full amount of the sale, an indicative amount of a Recurring Transaction or for a zero amount if no payment is being taken.
- Use appropriate data values (Stored Credential Indicators) to identify the initial storage of the credential and the subsequent usage of that stored credential.
    - If a payment is due at the time of the setup of the consent agreement, submit the initial transaction, either as a pre-authorisation or full financial transaction, with the correct data values.
    - If no payment is due at the time of the setup of the consent agreement, submit an Account Verification authorisation with the correct data values.

      Note: If the initial transaction is declined for any reason, the Stored Credential Indicator won't have been submitted and the credential shouldn't be considered stored.

    - All future transactions must then be submitted with the correct data values.

Note: For a CIT transaction, the cardholder identity must be validated before processing the transaction.

If you rent a terminal from us, no technical changes are required to add the data values. If you use the Global Payments E-Commerce Platform, transactions will include the correct data values. We'll advise you if any other technical changes are required to integrate with this service.

If your equipment or service is provided by a third party, please contact them to ensure the necessary data values are added. The technical information can be found in the *Stored Credential - Technical Implementation Guide* located on our website at **www.globalpaymentsinc.com/en-gb**. You'll find it in the Customer Centre under the option for Stored Credential Transactions.

The Consent Agreement

Disclosure and Cardholder Consent

Before storing the card details for future use, you, or a third party on your behalf, must establish an agreement with the cardholder**.**

Note: A separate consent agreement is not required for Industry Practice transactions. However, the possibility that these transaction types may be performed must be included in the original consent. For example, on hotel booking terms and conditions you'd need to disclose that the cardholder details will be used for No Show transactions.

The consent agreement must contain:

- A truncated version of the card number (i.e. the last four digits)
- How the cardholder will be notified of any changes to the consent agreement
- The expiry date of the consent agreement, if applicable
- How the stored card details will be used

In addition, if the cardholder is providing consent to you or the third party you're using to initiate transactions (MITs) using their card details, you must also include:

- Your cancellation and refund policy
- Your full postal address, including country and telephone number
- Transaction amount or how it will be calculated
- Any additional fees or surcharge, where permitted
- For Recurring Transactions, the frequency of the transactions

- For Instalments, the total purchase price and the terms of future payments, including the dates, amounts and currency
- For Unscheduled MITs, the event that will prompt the transaction.

Storage of the Consent

In all cases, card details must be stored securely. As part of your Card Processing Agreement with us you must be Payment Card Industry Data Security Standard (PCI DSS) compliant. For further details on PCI DSS, please refer to your *Merchant Operating Instructions*.

In addition, you must:
- Retain the consent for the duration of the agreement.
- Provide a copy to the cardholder.
- In the event of a dispute, provide a copy to the card issuer as evidence.

Consent Amendment or Cancellation

You or the third party you use must ensure that the following is adhered to:
- Notify the cardholder in the event of a change to the agreement
- In particular, provide notification for Recurring Transactions (seven business days) and Unscheduled MITs (two business days) before any of the following happen:
  - End of a trial period
  - More than six months have elapsed since the previous transaction
  - Any changes to the agreement, including date, amount, or how it's calculated

Don't complete a transaction:
- Beyond the duration of the consent as agreed with the cardholder
- If the cardholder requests that you or the third party you use change the payment method
- If the cardholder cancels the agreement in accordance with your cancellation policy
- If you or the third party you use receives a decline response

Note: For Instalment transactions, if the cardholder cancels in accordance with your cancellation policy, a cancellation or refund confirmation must be provided in writing within three days and a credit transaction receipt for the amount specified in the cancellation policy, if relevant.

Issued November 2020