Frequently Asked Questions – Credential on File Changes (Updated April 2019)

General Questions

1. **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.

2. **What's a tokenised card number?**
   Tokenisation is the process of replacing sensitive card data with a token value that retains all the essential information about the data without compromising its security. Since the token isn't a card number, it can't be used outside the context of a specific unique transaction with that particular merchant.

3. **Why are Visa and Mastercard making these changes?**
   Due to the increase in the number of transactions in which stored credentials are used, the Card Schemes want to be able to identify their storage and subsequent use to enable appropriate processing. This should lead to improved authorisation approval rates and completed sale transactions**.**

4. **Where can I find more information about stored credentials?**
   Please refer to the *Stored Credentials Guide* on our website at **www.globalpaymentsinc.co.uk** for further information. You'll find it in the Customer Centre under the option for Stored Credential Transactions.

5. **How do I know if this change impacts me?**
   This change will impact you if you store card details for future payments. You can also refer to the Decision Tree that can be found at the location detailed in Q4.

6. **What are the requirements/what changes do I need to make?**
   You, or the third party you use, must:
   - Obtain the cardholder's consent for the initial storage of their credentials, and
   - Use appropriate data values (Stored Credential Indicators) to identify the initial storage of the credential and the subsequent usage of that stored credential.

   Details of the consent agreement requirements can be found in our *Stored Credentials Guide.* The data value information can be found in our *Stored Credentials – Technical Implementation Guide.* Both can be found at the location detailed in Q4.

7. **When do the changes have to be made by?**
   All Stored Credential Transaction should already be flagged correctly, so if you haven't made these changes, you must do so immediately. Visa originally mandated **14th October 2017** as the official implementation date. However, they extended the date under a rule waiver until **April 2019**. Mastercard's implementation date was **13th April 2018** and will begin applying fines from **Q2 2019**. As the implementation dates have passed, any non-compliant merchants are potentially liable for fines from the Card Schemes.

8. **I currently complete transactions using stored credentials, what do I need to do?**
   You must start obtaining a consent agreement from any new customers before storing their card details, with immediate effect. You don't need to obtain a consent agreement for card details that you already use. In addition, all transactions processed using the stored card details, whether under a new or existing consent agreement, must contain the appropriate data values. As the Credential on File

© 2019 GPUK LLP. All Rights Reserved

implementation deadline has passed, if your transactions aren't compliant, card issuers can decline your transactions and you may be liable for any non-compliance fines levied.

9. What are the benefits to me of making this change?

Making these changes should result in higher authorisation approval rates and completed sales, as well an improved experience for your customers, with fewer complaints. It'll also allow you to avoid non-compliance fines levied by the Card Schemes.

10. What will happen if I don't implemented these changes?

Failure to implement the requirements may result in continued declined transactions and possible fines from Visa and Mastercard for not implementing the mandatory change. Correctly flagging Stored Credential Transactions initiated by yourself will also avoid the card issuer requesting Strong Customer Authentication (SCA) for the transaction (see the Strong Customer Authentication section below).

11. Are all card processors requesting their customers to make these changes?

Yes, this is a change mandated by Visa and Mastercard. All card processors in the UK and their customers accepting card payments are mandated to make the change.

12. What's a Cardholder Initiated Transaction?

A Cardholder Initiated Transaction (CIT) is any transaction where the cardholder is actively participating in the transaction. Please refer to the *Stored Credentials Guide* found at the location detailed in Q4. Card Holder Initiated Transactions are not exempt from SCA (see the Strong Customer Authentication section below).

13. What's a Merchant Initiated Transaction?

Merchant Initiated Transactions (MIT) are commonly initiated by a merchant without any active participation from the cardholder. There are two types of Credential on File MITS, Standing Instructions and Industry Practice Transactions. Please refer to the *Stored Credentials Guide* found at the location detailed in Q4. For SCA purposes (see the Strong Customer Authentication Section), a MIT is defined as any subsequent transaction where the amount can vary each time.

14. What are Standing Instruction MITs?

Standing instruction MITs are pre-agreed standing instructions from the cardholder for the provision of goods or services. The following transaction types are Standing Instructions transactions:

- Recurring Transactions
- Instalment Payments
- Unscheduled Credential on File Transactions.

15. What are Recurring Transactions?

Recurring Transactions are 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 (see the Strong Customer Authentication Section a Recurring Transaction must be the same amount every time.

16. What are Instalment Payments?

Instalment Payments are transactions that are processed on a regular fixed interval for a pre agreed amount for a single purchase of good 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. For SCA exemption purposes (see the Strong Customer Authentication Section), if the instalment amounts are the same every time, the transaction should be considered and flagged as a Recurring Transaction. If the instalment amounts aren't the same each time, it should be flagged as an MIT for SCA exemption purposes.

17. What are Unscheduled Credential on File Transactions?

Unscheduled Credential on File Transactions are 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.

18. What are Industry Practice Transactions?

Industry Practice Transactions are transactions that 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
- Resubmissions
- Reauthorisations
- Delayed Charges
- No Shows.

19. What are Incremental Authorisations?

Incremental Authorisations are 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. An example where this type of scenario is used is when a cardholder checks into a hotel and may have requested a room only and then subsequently adds 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.

20. What are Resubmissions?

Resubmissions are used when the original authorisation has been declined for insufficient funds. The cardholder will need to confirm that this is the case.

21. What are Reauthorisations?

Reauthorisations are used when the validity period for a previous authorisation has expired. Please refer to the *Stored Credentials Guide* found at the location detailed in Q4.

22. What are Delayed Charges?

Delayed Charges are 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 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.

23. What's a No Show?

No Shows are 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. They're typically in the hotel sector to cover lost revenue from guests failing to turn up.

Consent Agreements

24. When do I need to start requesting a consent agreement from a cardholder?

It has been a Card Scheme requirement since 14th October 2017 that you must establish an agreement with a new customer before storing their card details for future use.

25. What information needs to be included in the consent agreement?

Please refer to the *Stored Credentials Guide* found at the location detailed in Q4.

26. Do I need to obtain a new consent agreement for existing customers?

There's no need to obtain consent from your existing customers. However, any modifications to existing agreements, or new agreements undertaken, should adhere to the Credential on File rules with immediate effect.

27. How should I store the consent agreement?
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.

28. Where can I find more information about PCI DSS?
Please refer to your Merchant Operating Instructions, a copy of these can be found on our website at **www.globalpaymentsinc.co.uk**. You'll find this document in the Customer Centre under the option for Card Processing.

29. Previous letters and versions of the guides only refer to obtaining a consent agreement for Visa transactions. Do I need to make any changes for the other card types that I accept?
We recommend that you obtain a consent agreement for all the card details that you store for future use. This is good practice and will avoid any confusion and prevent errors.

Strong Customer Authentication

30. What's SCA?
From **14th September 2019**, a new regulatory requirement comes into effect that will impact the way payments take place. From this date, all payments will have to be validated using Strong Customer Authentication (SCA). SCA requires a cardholder to authenticate themselves for a transaction using at least two independent factors. These factors can be:

- Something the customer knows (for example a PIN number or password)
- Something the customer is (biometrics, such as a fingerprint or voice recognition)
- Something the customer is in possession of (for example a card or a mobile phone)

31. How do I implement SCA?
For ecommerce transactions, this can be achieved by using 3D Secure. For more details, please refer to the *PSD2 and Strong Customer Authentication Technical Implementation Guide*, which is on our website at **www.globalpaymentsinc.co.uk**. You'll find it within our Customer Centre, under the Strong Customer Authentication tile.

32. What's the difference between an authentication and an authorisation request?
An authentication request is how you verify the cardholder is the rightful owner of the card. It happens first before the authorisation request. In a face to face environment this would be by chip and PIN. In Ecommerce generally its 3D Secure, and a PSP will make that request for you. After the customer has been authenticated then you can request authorisation for the payment to be made.

An authorisation message is how you request payment for the goods or services that you sell. This is the message that you send to Global Payments that we forward on to the issuer (via the card scheme) on your behalf. The issuer approves or declines the authorisation.

33. Why is SCA relevant to Stored Credential Transactions?
While Stored Credential Transactions (also known as Credential on File Transactions) are out of scope for SCA as the cardholder isn't present to authenticate themselves, it's critical that these 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.

These transactions must be flagged both as a Stored Credential Transaction with one of two SCA exemption markers:

- a Recurring Transaction exemption (when the amount is fixed), or
- A Merchant Initiated Transaction exemption (any other Stored Credential Transaction where the amount varies)

34. When does SCA impact Stored Credential Transactions?
SCA is mandated by the Payment Services Directive 2 (PSD2) from **14th September 2019**. From that date, card issuers are obliged to seek SCA or decline transactions that aren't fully authenticated that should be. If the card issuer can't be sure that your transaction is exempt they will request SCA.

35. When do I need to perform SCA?

There are three scenarios when you'll need to perform SCA with a Stored Credential Transaction:

- The first transaction, when you store a cardholder's credentials for the first time, must be subject to SCA, either via 3D Secure for ecommerce or chip and PIN if it's performed in a customer facing environment
- All Cardholder Initiated Transactions should be subject to SCA or explicitly exempted
- If you incorrectly flag a Merchant Initiated Transaction and the card issuer can't be sure that it's exempt from SCA, then they may respond to the authorisation request with a return code value of 65 requesting you perform SCA. Until you do so, the authorisation request will be declined.

36. What about MOTO transactions?

Mail Order and Telephone Order (MOTO) transactions are out of scope for SCA. Provided that they're correctly flagged as MOTO and Stored Credential Transactions, both the first transaction, and subsequent (Customer Initiated Transactions) can be made by mail order or telephone order.

For subsequent Stored Credential Transactions that are merchant initiated (when the first transaction was performed by MOTO) then they should be flagged correctly – as Stored Credential Transactions and with a Merchant Initiated Transaction SCA Exemption Flag.

In all scenarios, it's important that the Scheme Reference Data from the initial MOTO transaction is stored and submitted with the subsequent transactions ensuring that the card issuer can trace the transactions back to the original one and know that it was an approved MOTO transaction.

37. What value should I authenticate when storing the cardholder's credentials?

This depends on why you're storing them. You can do an authentication for a zero amount if the final value isn't known. If you're storing the credentials for a known amount, for example to start an instalment plan, then the authentication amount should be the full amount not the individual payment amounts. If the cardholder doesn't recognise an authorisation amount (because it doesn't match the amount they were shown during authentication), then they can raise a dispute with their card issuer.

38. Where can I find more information about PSD2 and SCA?

Please refer to the *PSD2 and Strong Customer Authentication Technical Implementation Guide*, which is on our website at **www.globalpaymentsinc.co.uk**. You'll find it within our Customer Centre, under the Strong Customer Authentication tile.

Technical Changes

39. What technical changes do I need to make?

Any transactions processed using a stored credential, must contain the data values that are explained in the *Stored Credential -Technical Implementation Guide* located on our website at **www.globalpaymentsinc.co.uk**. You'll find it in the Customer Centre under the option for Stored Credential Transactions.

All Customer Initiated Transactions will be subject to SCA from 14th September 2019 and all Merchant Initiated Transactions will need to be flagged as SCA exempt to avoid card issuers challenging the transactions. The technical requirements for the changes needed are explained in *PSD2 and Strong Customer Authentication Technical Implementation Guide*, which is on our website at: **www.globalpaymentsinc.co.uk**. You'll find it within our Customer Centre, under the Strong Customer Authentication tile.

40. I rent a terminal from Global Payments, do I need to make any technical changes?

No, however, you'll still need to set-up a consent agreement with customers if you're storing card details for future use.

41. I use the Global Payments E-Commerce Platform, do I need to make any changes?

We've made the necessary technical changes to flow the correct data values for the Credential on File mandate and we'll be in further contact with you if you need to make any other changes for SCA. You

must implement the consent agreement requirements with immediate effect for any new customers where you're storing card details for future use.

42. **My equipment/service is provided by a third party/Payment Service Provider (PSP). Who do I need to contact to make these changes?**
    You'll need to contact the company that you have a contract with for providing your equipment/service to ensure they make the changes as soon as possible.

43. **What happens if my equipment provider/PSP can't make the changes?**
    It's very important that you contact your equipment provider/PSP as soon as possible so that they can make the changes required for you. They should be ready to support the Credential on File changes already and the new PSD2/SCA requirements from September 2019. They can contact us through their usual communication channel with us and schedule a time when they'll be able to complete their testing and implementations to meet all the mandates.

44. **Will I need to complete any testing before implementing the changes?**
    Yes, we recommend that you or your third party complete testing with us before the changes are implemented.

45. **Who do I need to contact to arrange the testing?**
    Testing can be arranged through your equipment provider/PSP or Relationship Manager.

46. **Will I incur a cost for making these changes?**
    This is something you'll need to ask your equipment supplier or PSP as your service contract is with them and not with us. If you rent a terminal from us or use the Global Payments E-Commerce Platform, then the changes we make will be done free of charge. If changes are required to your own equipment to integrate with our E-Commerce Platform, then you'll need to ask you supplier.

47. **Previous letters and versions of the stored credential guides only refer to the changes that need to be made for Visa transactions. Do I need to make any changes for the other card types that I accept?**
    Although our earliest communications only referred to Visa mandating the change, we've always recommended that changes were made for all card types. Mastercard followed Visa in mandating changes for Credential on File Transactions as well. To be fully compliant with both your Card Processing Agreement with us and the Card Scheme Rules, you must make the changes for both Visa and Mastercard. From the data we receive from you, we'll then flow the relevant data values as appropriate.

48. **Where does it say I have to make these changes?**
    Under the terms of your Card Processing Agreement with us, it is your responsibility to ensure that your card processing equipment meets industry standards. You can find further details on this in your Merchant Operating Instructions in the 'Using Your Own Equipment' section (on page 19). This states that "It is your responsibility to ensure that your card processing equipment meets industry security standards. You must carry out, and bear the cost of all upgrades to your equipment which we, or your terminal supplier, may reasonably request from time to time. This includes any developments required to meet changes to Card Scheme Rules. Failure to meet these changes will result in non-compliance with some of these regulations and may incur charges or penalties and increase your chargeback exposure."

    Also, in your Terms of Service under clause 12, we may vary your Card Processing Agreement to comply with Card Scheme changes to operating regulations, which you must adhere to. You can find a copy of the Terms of Service at: **https://globalpaymentsinc.co.uk/CPSD**. The Merchant Operating Instructions can be found on our website at **www.globalpaymentsinc.co.uk**. You'll find this document in the Customer Centre under the option for Card Processing.

49. **Where can I find more information about the technical changes that need to be made?**
    We've created a technical guide to explain the data values that need to be used for the initial storage of credentials and subsequent usage of them. The *Stored Credential - Technical Implementation Guide* and

the *Strong Customer Authentication Technical Implementation Guide* can be found at the location detailed in Q39.

50. Where do I get the technical specifications from to provide to my equipment provider/PSP?
The technical specifications are in the *Stored Credential - Technical Implementation Guide* and the *PSD2 and Strong Customer Authentication Technical Implementation Guide,* which can be found at the locations detailed in Q39.

Service. Driven. Commerce

Global Payments is HSBC's preferred supplier for card processing in the UK.

Global Payments is a trading name of GPUK LLP. GPUK LLP is authorised by the Financial Conduct Authority under the Payment Services Regulations 2017 (504290) for the provision of payment services and under the Consumer Credit Licence (714439) for the undertaking of terminal rental. GPUK LLP is a limited liability partnership registered in England number OC337146. Registered Office: Granite House, Granite Way, Syston, Leicester LE7 1PL. The members are Global Payments U.K Limited and Global Payments U.K.2 Limited. Service of any documents relating to the business will be effective if served at the Registered Office.
.