globalpayments®

3D SECURE AUTHENTICATION

MERCHANT COMPLIANCE GUIDELINES

SERVICE. DRIVEN. COMMERCE

CONTENTS

INTRODUCTION

3D Secure is a global e-commerce solution that enables cardholders to authenticate themselves to their card issuer through the use of a unique personal code. MasterCard SecureCode (SecureCode) and Verified by Visa (VbV) address current concerns about the security of online shopping and the high rate of e-commerce chargebacks. They're designed to take online shopping and consumer confidence to a new level.

Like chip and PIN authentication, the cardholder must enter their password in a separate browser window before their online transactions can be authorised. In seconds, the issuer confirms it's the true cardholder performing the transaction. Cardholders enjoy peace of mind knowing that no one else has access to their password. The participating merchant gets explicit evidence of an authorised purchase (authentication data).

Both SecureCode and VbV require 3D Secure Technology to be deployed on your website. This can be done by loading a Card Scheme registered Merchant Plug-In (MPI) application on your server. Alternatively, you can contract with a hosted service to perform the authentication process for you.

3D Secure is designed to help online merchants:

- reduce fraud
- reduce chargebacks
- increase online business
- increase cardholder confidence.

MasterCard have mandated that all ecommerce merchants accepting Maestro transactions must attempt to authenticate them using SecureCode. We recommend that you consider the implementation of VbV at the same time.

Failure to implement SecureCode on to your website means you can't accept any Maestro cards online. Processing Maestro without this could result in you being assessed for scheme penalties and fines. We'll be unable to defend these on your behalf and the penalties and fines will be passed on to you.

For further information on SecureCode and VbV, please access the respective Card Scheme websites at the following locations:

http://www.mastercard.com/uk/merchant/en/security/what_can_do/SecureCode/index.html

http://www.visaeurope.com/newsroom/infographics

MERCHANT BENEFITS

The primary benefit of 3D Secure is that the liability shifts from the merchant to the cardholder/card issuer on certain types of disputed online transactions. In a standard online transaction, when the cardholder or issuer disputes a transaction (as being fraudulent), the merchant is liable to pay back the disputed charges.

3D Secure addresses this problem and, in the majority of cases, shifts the liability to the cardholder/card issuer, provided the merchant and card processor are participating members of the scheme.

Once merchants have deployed 3D Secure, it's the card issuer's decision whether they choose to authenticate their cardholders for online transactions. The authentication data, together with an authorised approval, gives merchants a transaction that's guaranteed against the most common cardholder not present chargebacks – 'Cardholder not recognised' and 'Cardholder not authorised'.

Below is a table detailing the various permutations and shows where the fraud liability currently resides.

Merchant participating?	Card issuer participating?	Cardholder enrolled?	Global Payments participating?	Liability of chargeback falls on the following:
Yes	Yes	Yes	Yes	Cardholder
Yes	Yes	No	Yes	Cardholder
Yes	No	No	Yes	Card issuer
No	Yes	Yes	Yes	Merchant
No	No	No	Yes	Merchant

Another benefit from implementing 3D Secure is the assurance merchants can provide to their customers who are considering ecommerce transactions. For those cardholders that are afraid to shop online due to security concerns, authenticated payments may convince prospective shoppers that it's safe to use their card online. Seventy-three percent of consumers surveyed by MasterCard state that enhanced security would influence their decision to purchase online (information publicly available on the MasterCard website).

THE POWER OF THE SECURECODE MARK AND THE VBV LOGO

MasterCard.
SecureCode.

Verified by
VISA

By displaying the SecureCode mark and the VbV logo, displayed above, on your website, particularly at the checkout page, you can let your customers know you're working to make their internet shopping experience safer.

We'll provide you with these once you've implemented your 3D Secure solution, and testing and accreditation is complete.

HOW IT WORKS

The cardholder authentication process enables the card's issuer to confirm to you that they've checked the cardholder's identity while the transaction is taking place. This process is controlled by a piece of software that's installed on your website known as a Merchant Plug-In (MPI), which communicates directly with MasterCard and Visa for all the card issuers who participate in this service.

Once the secure authentication has been received back from the card issuer, the payment transaction proceeds in the usual way. You must also ensure that additional security data is included in your request for authorisation (to indicate the status of the transaction). This will ensure you're protected from liability should the transaction be denied by the cardholder.

THE PROCESS FLOW

1. The cardholder enters their card details in the checkout page.

2. Your MPI contacts either the MasterCard or Visa Directory to check for the card issuers' participation.

3. The directory responds either 'Yes' (go to next step) or 'No' (go to step 6).

4. If the card issuer chooses to authenticate the cardholder, a space appears on your website for the cardholder to input their password or enrol during shopping (go to next step). If the card issuer chooses not to authenticate the cardholder, go to step 6.

5. The card issuer validates the password and sends an authentication response back to your MPI.

6. Your system then requests authorisation in the usual way, but containing the additional authentication data.

AUTHENTICATION FAILURE

Whilst registered cardholders should become familiar with the process, instances of authentication failure may still arise for the following reasons:

- the cardholder may enter their password incorrectly (a maximum of 3 attempts are usually allowed)
- the authentication window may time-out and take the cardholder back to your checkout screen
- the cardholder may close the authentication window.

If a registered cardholder's identification details aren't approved, you shouldn't continue with the transaction. Your normal operational practices should then determine how you proceed, which may include asking for an alternative means of payment instead.

MERCHANT IMPLEMENTATION

Before you can start using your 3D Secure solution, testing has to be completed by MasterCard, Visa and/or Global Payments. We'll need to establish whether MasterCard and/or Visa have already accredited the solution via another card processor or whether this is the first approach for accreditation.

The following sections highlight the level of testing required for each implementation type.

GLOBAL IRIS IMPLEMENTATIONS

If you're using our Global Iris Remote facility, you need to make sure you've also completed the required MPI integration. If you're using our Global Iris Re-direct facility, the MPI is already pre integrated.

Please contact the Global Payments helpdesk to discuss further on 0345 702 3344*, selecting the option for Global Iris enquiries. Lines are open 8:30 am to 6:15 pm Monday to Friday, excluding Eire public holidays.

No other testing is required by us.

APPROVED THIRD PARTY BUREAU IMPLEMENTATIONS

If you use the services of a third party bureau to host your web solution you'll need to contact them and discuss the implementation of 3D Secure on your website. Most of the larger bureaus have a pre-approved Global Payments and Card Scheme registered solution which will require no further testing.

The third party won't be required to undertake Visa Product Integration Testing (PIT) testing again with us if they've already been accredited by another card processor.

The third party bureau must send us:

- a copy of Visa's letter of confirmation issued after successful PIT testing
- an email stating that since accreditation with their first acquirer the only changes to be made to the MPI will be the card processor BIN, the URL to where the messages will be sent and the merchant numbers.

MERCHANT/UNAPPROVED THIRD PARTY BUREAU IMPLEMENTATIONS

If you've developed and manage your own web solution, you'll need to purchase a Card Scheme registered MPI. A list of these is detailed on:

www.mastercard.com/uk/merchant/en/security/what_can_do/SecureCode/vendors.html

This will require additional testing by us.

Our testing is to ensure that your systems can connect into our card processing service and the data can be processed accordingly. In the case of SecureCode and VbV, the 'authentication' process falls outside the card processor's functionality, hence it is assumed that the merchant can 'simulate authentication' and generate the values to be populated in the auxiliary data fields of the authorisation request. If this isn't feasible, an alternative would be to arrange to test via the Card Schemes test facilities with all associated costs being met by you. If testing is via the Card Schemes, this may impact testing timescales as formal test slots will need to be arranged. Our testing is therefore based on the assumption that you can 'simulate authentication'. If testing is completed via Card Schemes, you'll be provided with the relevant test script specific to the respective scheme. However, at some stage during the testing with Card Schemes, you'll need to link to our test host for the authorisation request/response to complete the SecureCode accreditation with us.

If this is your first attempt at accreditation, we must refer you to MasterCard and/or Visa's website to obtain the necessary details to commence compliance testing. Once this is complete we must see sight of the accreditation letter from MasterCard and/or Visa's compliance testing **before** any other testing is undertaken.

Once accredited by MasterCard, our own testing can commence.

Once accredited by Visa, further Visa PIT testing is required before our own testing can commence.

1. Ensure that you book your Visa's PIT testing 3 days in advance of the pre-production testing.

2. Once you've completed PIT testing, a Review Test Activity Report will be produced. This is forwarded to Visa (serviceimplementation@visa.com) by you/the third party bureau, who'll then audit the PIT testing. If successfully completed, Visa will issue a confirmatory letter.

3. You must then send us a copy of Visa's letter of confirmation issued after successful PIT testing.

4. Book Global Payments' test system at least 1 day in advance of the end to end certification for the duration of 1 working day using our test Merchant ID, which will be provided to you.

5. End to end certification testing at your site will take approximately 1 day and will require you to have obtained and recorded the additional Cardholder Authentication Verification Value (CAVV) fields from MasterCard and/or Visa used during compliance testing. Once authenticated and captured, the CAVV will then be passed onto us during On Line Authorisation (OLA) testing to ensure that all data is passed to/from you as required by the Cards Schemes and our systems. It won't matter for testing purposes that the CAVV used won't be the actual value for the card used. The purpose of this test is to ensure that the CAVV data is being passed to us in the correct message format.

6. Once our testing has been undertaken you should obtain a copy of a screen print of the file log showing the additional auxiliary data in the formatted message. This screen print can be obtained up to 7 days after the testing has been completed. You should also receive a file with the transactions from the test script.

Note: There's an accreditation and registration charge that will be discussed with the Sales Manager, who'll confirm the cost to you.

INLINE AUTHENTICATION WINDOW

When implementing 3D Secure, you've two options in the way you can configure the authentication windows – that is, pop-up windows or inline windows.

With pop-up authentication windows, research has shown that cardholders often mistake a new window as an advertising message and will often close it without checking. In addition, cardholders with slower connections to the internet are even more likely to close pop-up windows, often doing so before the window has completed loading in the browser.

Closing a pop-up authentication window in this way can impact the authentication process, cause unpredictable results and adversely affect the cardholder experience. One of the key lessons learned is that the window closure rates are substantially less with the inline authentication window.

In addition, as the rate of pop-up advertising has increased, pop-up suppression software (sometimes referred to as ’Pop-up Killers‘) has gained increased market awareness and usage. Such software doesn’t only occur in stand-alone applications, but some browsers and online service providers have begun to incorporate pop-up suppression as a standard feature of their service.

We strongly recommend that you configure the authentication page as an inline window.

Important aspects to consider when deciding on frame inline or full inline:

- full inline has the benefit of a similar implementation and less scope for misunderstanding and mistakes
- frame inline displays the authentication page in your main window with your header. Therefore, 3D Secure is seen as a natural part of the transaction process. It’s recommended that the top frame includes your standard branding.

Frame inline implementation must also:

- provide enough screen space for the window to fit in. The recommendation is to use a top frame only in order to have a less ’crowded‘ screen
- ensure that the authentication window is not pushed out of the viewable area for low resolution screens
- ensure that the frame doesn’t include any other links or exit points that may distract the user from conducting the authentication process (such as ’search‘ options, standard navigation menu, etc)
- avoid using the HTML element iframe which can cause compatibility issues
- ensure that all frames must be of HTTPS type. Avoid mixing HTTP and HTTPS
- provide simple, correct instructions and allow cardholders an easy way to go back.

ACTIVATION DURING SHOPPING

Activation During Shopping (ADS) gives cardholders the opportunity to enrol in SecureCode or VbV while they're shopping at a participating merchant. This innovative approach allows participating issuers the ability to deliver an activation message to any of its cardholders. The message is sent by the issuer and generally they'll allow the cardholder to decline registration for a number of transactions before they'll enforce registration. Each issuer is tackling registration in a different way.

ADS works exactly the same as the 3D secure password authentication window. An inline window will appear prompting the cardholder to enter three pieces of authenticating data plus their email address. The issuer won't use the email address for identity verification. This page may also include links to pages for their Privacy and Security policy and Terms and Conditions.

Having entered this identity information, the cardholder selects 'activate now'. The issuer verifies the cardholder's identity and, if successful, the process moves on to a password creation stage.

A further 'create your password' inline window will appear. Here the cardholder creates a password then re-enters the password to confirm the correct entry. After successfully creating a password, the cardholder is enrolled in the service with their card issuer.

IMPLEMENTATION – BEST PRACTICES

PRE-MESSAGE NOTIFICATION

Pre-message notifications increase cardholder awareness and prepares the cardholder for the next screen to be displayed. It’s best to include generic text and not to make any assumptions that might confuse cardholders.

SECURECODE AND VBV LOGO

The authentication process is more successful and flows more smoothly when the SecureCode and VbV logos are included on your website, particularly at the checkout page.

BACK BUTTON FUNCTIONALITY

If your site allows the use of the ‘Back’ button, verify that it functions properly and test it thoroughly. Analysis has shown that some inline deployments don’t function properly when a cardholder clicks the Back button. In some cases, when the Back button is clicked, an alert is presented warning that the previous page has expired. Some cardholders may close the window if they see this message. You should ensure that your inline deployment responds accordingly when the cardholders click ‘Back’. This feature should also be fully tested.

FREQUENTLY ASKED QUESTIONS

What’s 3D Secure?
3D Secure is the generic terminology that covers both MasterCard’s (SecureCode) and Visa’s (Verified by Visa) version of the additional cardholder authentication service for ecommerce transactions.

What’s MasterCard SecureCode and Verified by Visa (VbV)?
MasterCard SecureCode and Verified by Visa are programmes designed to provide online merchants with the added security of having card issuers authenticate their individual cardholders and qualify their online transactions for protection against ’cardholder not authorised‘ or ’cardholder not recognised‘ chargebacks.

Is there any additional cost to process using this authentication method?
3D Secure is provided free of charge with the Global Payments’ Global Iris service. If you use the services of a third party bureau, then you should discuss the cost of implementation with them.

How does 3D Secure work?
When a cardholder submits their online order at a participating merchant, the MasterCard SecureCode/Verified by Visa solution performs the following to ensure that the cardholder is authorised to make this transaction:

- it initiates an inline window from the card issuer prompting the cardholder to enter their unique personal code
- the issuer validates the personal code and approves the transaction.

I use the Global Payments’ Global Iris Remote service; do I have to do anything?
Yes, you must make sure that the 3D Secure service (MPI) has been integrated into your system.

I use the Global Payments’ Global Iris Re-direct service; do I have to do anything?
No, the 3D Secure service (MPI) has already been automatically integrated into the Re-direct service.

I use a third party bureau for my website, what do I need to do?
If your website isn’t already 3D Secure enabled you should contact your solution provider and request they provide you with the facility to process transactions with this additional authentication.

I have developed my own website and submit directly into Global Payments, what do I have to do?
You need to purchase a Card Scheme registered MPI (Merchant Plug In) from a certified 3D Secure vendor and integrate it into your website. Testing is then required with Global Payments.

How do I find a certified 3D secure vendor?
A current list of certified compliant MasterCard SecureCode vendors is available on the MasterCard Merchant website.

www.mastercard.com/uk/merchant/en/security/what_can_do/SecureCode/vendors.html

What steps do I need to take to support 3D Secure?

As an online merchant, all you need to do is:

- install a Card Scheme registered MPI (Merchant Plug In) on your site. This may already be available to you if you use our Global Iris service
- transmit transaction authentication values to the card issuer via your normal authorisation process using the Universal Cardholder Authentication Field (UCAF).

How do I benefit from using 3D Secure on my website?

- Protection from ‘cardholder not authorised’ chargebacks for fully compliant transactions. This protection is designed to reduce your chargeback exposure and processing expenses.
- Consumer confidence increases, making customers more likely to make a purchase on your website.
- You expand the geographic reach of your business by selling to customers in countries where online debit cards are used more widely than credit cards. In addition to added protection against chargebacks for these customers, you will be able to process their Maestro debit transactions.

Does MasterCard SecureCode also support Maestro cards?

Yes. MasterCard SecureCode provides a way for issuers to support Maestro debit transactions over the internet. This allows more cross-border transactions from countries where debit is more established than credit.

Am I required to display the MasterCard SecureCode programme mark and the Verified by Visa logo on my site?

Yes, once you have successfully completed testing the logos must be displayed. This lets your customers know you are doing your part to make their transactions safer.

What happens if I don’t implement MasterCard Secure Code?

As MasterCard have mandated the use of SecureCode with all Maestro transactions, you must remove all reference to Maestro from your website, you mustn’t display the Maestro logo and you must stop accepting Maestro cards for payment. If you continue to accept Maestro, you may be liable for significant financial penalties for non-compliance.

USEFUL CONTACT DETAILS

MASTERCARD

http://www.mastercard.com/uk/merchant/en/security/what_can_do/SecureCode/index.html

VISA

http://www.visaeurope.com/receiving-payments

GLOBAL IRIS

New sales/enquiries about our Global Iris service

Call 0800 731 8921*. Lines are open 9:00 am to 5:00 pm Monday to Friday, excluding public holidays.

Technical help for existing Global Iris customers

Call 0345 702 3344*, selecting the option for Global Iris enquiries. Lines are open 8:30 am to 6:15 pm Monday to Friday, excluding Eire public holidays.

Or email globaliris@realexpayments.com.

*To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide a Textphone service on 0345 602 4818.

Global Payments
51 De Montfort Street
Leicester
LE1 7BB
Tel 0345 702 3344
Textphone 0345 602 4818
www.globalpaymentsinc.co.uk
www.globalpaymentsinc.com

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 2009 (504290) for the provision of payment services.

GPUK LLP is a limited liability partnership registered in England number OC337146. Registered Office: 51, De Montfort Street, Leicester, LE1 7BB. 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.