Internet Authentication Procedure Guide

Authenticating cardholders successfully

V10.0 Released May 2012

Software Version: Internet Authentication Protocol

barclaycard

Doc Version Control		
Version No.	**Date Issued.**	**Reason for Change**
3.0	July 2005	Additional Appendix – Best Practice guide Additional Visa chargeback reason code Card types not supported to include Maestro
4.0	June 2006	New Visa logo
5.0	October 2006	MasterCard SecureCode™ liability shift revisions Revised contact times
6.0	August 2007	Maestro liability shift inclusion
7.0	October 2007	Liability shift changes
8.0	March 2009	Re-brand
9.0	August 2010	Inclusion of Barclaycard SmartPay
10.0	May 2012	Update in regard to upgrade of ePDQ platform

Contents

Glossary & Terminology

3D Secure	3 Domain Secure. E-commerce environment including Acquirers/Merchants, Issuers/Cardholders and Card Schemes.
AAV	Accountholder Authentication Value. Unique reference generated by MasterCard and Maestro card issuers to prove authentication took place.
ACS	Access Control Server. Card Issuer system to record which cardholders are registered.
APACS	Association of Payment And Clearing Services. Industry body supplying authorisation and clearing payment file formats.
BIN Cache	A record of issuer BIN ranges stored locally on your authentication system.
CAVV	Cardholder Authentication Verification Value. Unique reference generated by Visa card issuers to prove authentication took place or was attempted.
CRReq	Card Range Request. 3D Secure Protocol message type.
CRRes	Card Range Response. 3D Secure Protocol message type.
ECI	eCommerce Indicator. Provides the security level used in an internet transaction.
ePDQ	Barclaycard Payment Acceptance secure online payment service.
HPP	ePDQ Hosted Payment Page.
API	ePDQ Application Programme Interface.

European Region	Specific European regions as defined by the card schemes (see Intra-Regional).
IAV	Issuer Authentication Value. Generic term that corresponds to either the Visa CAVV or MasterCard AAV.
Inter-Regional	The region defined by the card schemes that includes issuers outside of the "local region". For UK merchants these will include Asia, USA and Australia amongst others.
Intra-Regional	The region defined by the card schemes as the "local region". For UK merchants this will include UK and most European countries.
IPOS	Integrated Point of Sale. Also called Host to Host.
ISP	Internet Service Provider.
MasterCard Directory	A system operated by MasterCard which determines whether a specific issuer and card number is participating in authentication, and if so, it returns the URL of the appropriate Access Control Server to the Merchant Plug-in.
Merchant Plug-in	Generic term to describe the SDK.
PAReq	Payer Authentication Request. 3D Secure Protocol message type.
PARes	Payer Authentication Response. 3D Secure Protocol message type.
Pop Up	Internet Browser Pop Up window, displayed within the main browser page.
PSP	Payment Service Provider. Companies who offer internet transaction routing to acquirers.

Rest of the World	International, non-European region (see Inter-Regional).
RFI	Requests for Information. Also known as retrieval. A separate process to a chargeback used by card issuers to obtain further transaction information.
SDK	Software Developers Kit.
SecureCode™	SecureCode™. Cardholder authentication scheme for MasterCard and Maestro cards.
Barclaycard SmartPay	Barclaycard Payment Acceptance secure online payment service.
T&E	Travel & Entertainment.
UCAF	Universal Cardholder Authentication Field. The data field used by MasterCard and Maestro issuers to send the AAV (see above).
VbV	Verified by Visa. Cardholder authentication scheme from Visa.
VEReq	Verify Enrolment Request. 3D Secure Protocol message type.
VERes	Verify Enrolment Response. 3D Secure Protocol message type.
Visa Directory	A system operated by Visa which determines whether a specific issuer and card number is participating in authentication, and if so, it returns the URL of the appropriate Access Control Server to the Merchant Plug-in.
We, us, our	Barclays Bank PLC.
XID	Transaction Identifier.

You, your	The person, people or organisation shown as the merchant or any agent or sub-contractor we have approved. If two or more people are shown as the merchant each of you is liable to us individually as well as jointly.

Introduction

This procedure guide gives you all the information you need to use for internet cardholder authentication. It details your roles and responsibilities, our roles and responsibilities and some key information required by supported card schemes.

The following card scheme authentication services are offered by us and covered by this procedure guide:

Verified by Visa (Visa)

SecureCode™ (MasterCard and Maestro)

We will only process authentication transactions submitted by the above schemes, and for services that we have mutually agreed you will use.

This procedure guide should be used in conjunction with your Merchant Agreement(s), Terms & Conditions, Accepting Cards Procedure Guide and the Hosted Payment Page (HPP) Barclaycard SmartPay Integration Guides or Software Development Kit integration guide as appropriate.

Using your procedure guide

Your procedure guide is divided into sections to clearly provide information that allows you to use the Authentication service effectively. There are two general sections that must be read (Authentication Information & Card Scheme Compliance) and five specific sections which should be read dependent on which payment product you are using. The sections are broken down into:

Authentication Information
This provides general operational and technical information that you must understand before using any Authentication service. Where applicable we have indicated whether you have any responsibility.

You must read "Section 1 – Authentication Information" section.

ePDQ HPP Users
As the authentication process within the ePDQ HPP is maintained and controlled by us you have no direct responsibility for ensuring compliance with the card schemes.

If you are using the ePDQ HPP, you must read "Section 2 – ePDQ HPP Users".

ePDQ API, PSP or IPOS Users connecting to the Barclaycard Payment Acceptance Hosted Authentication service
If you connect to the Hosted Authentication service, we will maintain a degree of control over the process for authentication of transactions. You must ensure that you understand your requirements to connect to the service.

If you are using the ePDQ API, PSP or IPOS system, you must read "Section 3 – Hosted Service Users".

Barclaycard SmartPay Hosted Payment Page Users
As the authentication process within Barclaycard SmartPay is maintained and controlled by us you have no direct responsibility for ensuring compliance with the card schemes.

If you are using the Barclaycard SmartPay Hosted Payment Page, you must read "Section 4 – Barclaycard SmartPay Hosted Payment Page Users".

Barclaycard SmartPay API Users
As the authentication process within Barclaycard SmartPay is maintained and controlled by us you have no direct responsibility for ensuring compliance with the card schemes. You will however need to ensure that:

1. **Your processing account is configured by Barclaycard SmartPay to support 3D Secure.**

2. **Your software supports redirecting the shopper to the card issuer and submitting a second API call to complete the payment.**

If you are using the Barclaycard SmartPay API, you must read "Section 5 – Barclaycard SmartPay SPI Service Users".

Contacting us

Direct to Card Schemes

If you have chosen to connect direct to the relevant card schemes using your own or a third party (i.e. non-Barclaycard Payment Acceptance) authentication solution you must be aware of your responsibilities.

If you are going to connect direct to the card schemes, you must read "Section 6 – Direct to Card Schemes".

Card Scheme Compliance

The final section of your procedure guide details the responsibilities you have to ensure you remain compliant with the card schemes offering cardholder authentication.

You must read "Section 7 – Card Scheme Compliance" section.

E-commerce Support Team

Contact us on **0844 822 2099****

Monday to Sunday: 8.00am to midnight

Alternatively you can email us at: **epdq@barclaycard.co.uk**

Barclaycard SmartPay Support Team

For Barclaycard SmartPay contact us via email at:

support.smartPay@barclaycard.co.uk

Alternatively you can call us on the following:

From the UK – **01604 269518***

Outside the UK – **+44 1604 269518***

Support hours:
Monday to Sunday: 8.00am to midnight GMT

*Calls may be monitored and/or recorded to maintain high levels of security and quality of service

Section 1 – Authentication Information

The following section must be read by all users of the authentication service and provides the requirements, responsibilities and policies relating to usage of the service.

You may find it useful to reference the index at the front of this procedure guide to locate a particular subject or reference point.

You should ensure that you are familiar with how authentication works before using any of the services. It is important that you understand the 3D Secure protocol supporting authentication. Information on this will be available within your authentication software integration guide or can be found on the Barclaycard Payment Acceptance website.

1.1 The Key Benefit of Authentication: Liability Shift

Internet transactions have historically carried a higher risk than standard "High Street" transactions. This is because neither the cardholder nor the card can be positively identified at the time of purchase. In the event that a card was used fraudulently or the cardholder disputed the transaction, the card issuer would charge the transaction back to us.

If we receive a chargeback for a transaction processed by you we will request evidence to support the validity of the transaction. In most cases evidence can be provided that the card was used, but not that the **genuine cardholder** was using the card. In this scenario, the Card Issuer would charge the transaction back to you (a chargeback), resulting in the loss of goods/services plus the cost of the transaction.

The introduction of cardholder authentication means that you will now have the ability to prove that the cardholder used their card at the time of transaction.

Cardholder authentication helps prevent chargebacks where cards are used fraudulently, or where the cardholder denies using the card. The liability shifts from you, back to the card issuer.

Minimising the risk of fraud is essential and Internet Authentication should be used in conjunction with and not instead of any other fraud checks that you should have in place and it is important that you maintain your existing fraud checks. Failure to maintain your existing fraud checks could result in you receiving chargebacks. Please refer to Appendix B for our 'Best Practice' on managing internet fraud.

1.2 What's changed?

The table below shows how your business may benefit from using cardholder authentication.

Transaction Type	Internet	Internet
Responsibility to check cardholder	You (Merchant)	Card Issuer
Responsibility for transactions where cardholder denies using their card (subject to specific conditions – see Appendix A)	You	Card Issuer
Responsibility for other chargebacks (i.e. non-delivery of goods/services)	You	You

Cardholder authentication protects you against specific types of chargeback. These are detailed below and were correct at date of publication. You will be notified if there are any changes to this.

1.3 Chargeback Reason Codes Included

You must be aware that each card scheme uses a different "reason code" to charge a transaction back. If you are using any automated risk tools you should ensure you cater for each scheme reason code where applicable.

Visa:

75	Transaction not recognised – when the cardholder advises that they do not recognise an item on their card statement. This does not apply to transactions with an ECI 5 or 6 value.
85	The card was NOT present and a transaction was processed without cardholder permission, or a fictitious (card) account number was used and transaction was not authorised (a fraudulent transaction).

MasterCard:

37	The cardholder denies responsibility for the transaction or the acquirer lacks evidence of a cardholder's authentication (i.e. signature).
63	When a cardholder claims he or she does not recognise a non face-to-face transaction (such as an eCommerce transaction). If after being presented with new information, the cardholder asserts that he or she did not authorise the transaction. **Note**: You may be asked to provide supporting information to us to defend a transaction (see section on Retrieval Requests). Protection against this reason code may help to avoid a chargeback following such a request.

Maestro:

22	Cardholder Not Present Transaction not initiated by a bona fide cardholder.

One of the critical success factors of the authentication schemes is to remove chargebacks from the system. Each of the card issuers are adding edits to ensure, wherever possible, that you are not charged back for a transaction that was authenticated.

There are certain scenarios where you may not benefit from liability shift. This is typically due to regional variations in card scheme rules and is detailed under Appendix A – Liability Shift Rules.

Please note: You do not benefit from liability shift for any other chargeback reason codes other than those defined in this document.

1.4 Full Authentication versus Attempted Authentication

To support authentication by acquirers and issuers, the card schemes have introduced two types of authentication. These help to identify which level of authentication was used, and what liability shift is available.

Full Authentication

This occurs when the card issuer, cardholder, merchant and acquirer all correctly process an authentication transaction. The cardholder will successfully authenticate himself or herself (through a browser pop up or in-line window) with their card issuer. This is often known as "Full Authentication" for Visa and "Full UCAF" for MasterCard.

The card issuer will provide an IAV (Issuer Authentication Value) to indicate authentication took place. This value is passed in the authorisation process as proof of authentication.

Attempted Authentication

This occurs when the cardholder is not registered for authentication, but you are submitting an authentication request. In this instance, the issuer may still provide an IAV (sometimes referred to as an "Attempt") to indicate that you successfully tried to authenticate the cardholder.

The card schemes differ with their support of attempted authenticated transactions.

For Visa:

The definition of an attempted authentication for Visa cards is when both the Merchant (you) and the Acquirer (us) support Authentication and can confirm that everything has been integrated correctly. The attempt to authenticate must be successful. The card issuer must return a response confirming the attempt. If the card issuer is unable to confirm the attempt (e.g. the system went down) then you are unable to claim attempted authentication.

A successful attempt for Visa includes:

Confirmation that the Issuer is not participating, from the BIN Cache or Visa Directory

Confirmation that the cardholder is not participating or has not yet enrolled

A 3D Secure response of "A" in the PARes.

Visa card issuers must send an IAV for successfully authenticated transactions and may optionally send an IAV for a successfully attempted authentication.

For MasterCard and Maestro:

The definition of an attempted authentication for MasterCard and UK issued Maestro cards is when both the Merchant (you) and the Acquirer (us) support Authentication and can confirm that everything has been integrated correctly. The attempt to authenticate must be successful. The card issuer must return a response confirming the attempt. The term for this is "Merchant UCAF" which simply means that you are participating in the SecureCode™ scheme.

You can claim attempted authentication on a MasterCard and UK Maestro SecureCode™ transaction when you make any attempt to authenticate the cardholder. Ideally, you should receive a 3D Secure message response from the card issuer confirming the attempt but if not, you can still claim liability shift as long as you have correctly integrated the SDK and successfully sent the authentication request. This means that liability shift may be offered for MasterCard and UK Maestro when:

You receive confirmation that the Issuer is not participating, from the BIN Cache or MasterCard/Maestro Directory

You receive confirmation that the cardholder is not participating or has not yet enrolled

The cardholder pop up or in-line window does not appear due to Issuer/Cardholder error

The issuer service is not responding to your authentication request

Authentication fails, but the transaction is authorised by the Card Issuer.

MasterCard/Maestro issuers do not currently send an IAV for a successfully attempted authentication.

Whether you gain "Full UCAF" or "Merchant UCAF" depends on the MasterCard or Maestro equivalent of the ECI. This must be passed in your payment solution to ensure the correct liability shift is obtained.

You cannot claim attempted authentication on a SecureCode™ transaction for internationally issued Maestro cards.

1.5 Levels of Liability Shift Protection

Depending on where the card is issued, and the type of authentication gained (see above), liability shift can differ. Any liability shift is subject to strict adherence to the 3D Secure protocol. The following provides a summary.

For Visa:

- Full global cover (Visa Intra and Inter Regional) for fully authenticated and successfully attempted authentication.

MasterCard:

- European Region cover for both full and successfully attempted authentication

- Global cover for both full and successfully attempted authentication.

(**Note**: MasterCard applies different rules for Commercial cards. Please see section 1.7 below.)

Maestro:

(**Note**: Maestro applies different rules for UK and Internationally issued cards.)

- Global cover for full authentication
- Successfully attempted authentication for UK domestic transactions where both the Card Issuer and the Merchant are located in the UK.

1.6 Card Types Supported
The following card types are supported by each card scheme for cardholder authentication.

Verified by Visa:

Visa Credit

Visa Debit

Visa Electron

Visa Commercial

SecureCode™:

MasterCard Credit (including Commercial cards)

Maestro

1.7 Card Types Excluded
Verified by Visa:

Visa Commercial (Non-European Card)

The Visa card scheme currently excludes the above from any form of chargeback liability shift. Visa has issued the following to cater for this exclusion:

"Issuers receiving a 3D Secure Authentication Request for inter-regional transactions using a Commercial Card... must respond to the request with an "Unable to Authenticate" response. The merchant may proceed with the transaction, but will identify it with ECI 7 in the clearing record"

OR,

"For a commercial card transaction for which a (correct) CAVV was sent, the CAVV Validation service will send a CAVV Response Code of "B" in field 44.13 to the Issuer and Acquirer. For inter-regional transactions this is defined as "CAVV passed validation – information only, no liability shift".

SecureCode™:

MasterCard Commercial (International cards)

1.8 Pop up or In-Line window?
When Internet Authentication was first launched, most solutions used a browser pop up window to display the card issuer authentication page.

Research has been undertaken by the card schemes to identify any problems relating to cardholders closing the window believing them to contain advertising. There was also the risk that the cardholder's browser may have built in pop up killers/blockers to stop the window appearing.

As an alternative to pop up windows, you are able to use an in-line window. This will generate the card issuer details in a full frame page. You may also display the page within a frame and display your logo at the top, or side. Full details of in-line options are provided in the SDK integration guide.

Please note that the ePDQ HPP and Barclaycard SmartPay Hosted Payment Pages use an in-line window and control the display of the window automatically on your behalf. This cannot be altered.

1.9 How do I use the service?
You must have a valid internet merchant relationship with us to take full advantage of the service.

You must be registered with us to use cardholder authentication services and have integrated the authentication software into your chosen payment solution. Unless you specifically request an alternative, we will assume you wish to use authentication for all participating card schemes supported by us.

The following options are available to you:

1. **Use our integrated Hosted Authentication service and ePDQ HPP**

2. **Use our integrated Hosted Authentication service and Barclaycard SmartPay**

3. **Connect to our Hosted Authentication service using our SDK**

4. **Source or develop your own 3 Domain Secure Authentication software solution, which must comply with the 3D Secure specification of at least protocol level 1.0.2.**

The ePDQ HPP, SDK and our Hosted Authentication service are fully compliant with the protocol level 1.0.2.

If you have chosen to source your software from a third party vendor, that vendor will need to have been approved by all participating card schemes supported by us. You can find details of approved vendors, complete with product version at **www.visaeu.com/verifiedbyvisa** for Visa (refer to the "How does it work" section) and **www.securecode.com** for MasterCard and Maestro.

Section 2 – ePDQ HPP Users

You must read this section if you are using the ePDQ Hosted Payment Page (HPP) with integrated cardholder authentication.

The ePDQ HPP is a fully hosted payment and authentication service. If you use the HPP you will not have to integrate any additional software for cardholder authentication. Once you have successfully applied for the service we will activate the HPP to perform authentication on all relevant transactions.

Although the ePDQ HPP requires no specific authentication integration, you must ensure that you have correctly integrated the ePDQ HPP in line with the instructions provided to you. Failure to do this may result in incorrect transaction processing.

2.1 Your Responsibilities
We control the authentication process within the HPP and will ensure you have minimal disruption to your current transaction processing. You must:

- **Correctly integrate the ePDQ HPP in line with instructions provided at sign up**

- **Read and understand how the HPP handles authenticated transactions – this information is provided in the integration guide**

- **Set the "Continuity Options" within the ePDQ appropriately to suit your risk policy**

- **Request Activation of the ePDQ**

- **Advise us immediately if you cease using the ePDQ HPP**

  – Check to ensure the correct Authentication values are associated with your transactions
  – Please check Transaction Detail report in your ePDQ Store Administration Tool for details.

2.2 Our Responsibilities
We will:

- **Register you with each participating card scheme supported by us**

- **Provide you with the ePDQ HPP integration guide**

- **Control the processing of authentication transactions**

- **Adhere to relevant card scheme policies**

  – Process transactions accordingly for "failure" scenarios in line with your configuration requirements for the ePDQ HPP

  – Maintain a full audit trail and provide transaction evidence to the card issuer in the event of a chargeback where we believe authentication was correctly performed and where liability shift is available (this does not include Retrieval Requests (RFI), see section 7.5)

  – Ensure the correct authentication values are attached to both the authorisation and clearing message where appropriate.

2.3 Transaction Records

We will maintain authentication transaction records on your behalf and will use these to provide evidence that the transaction was authenticated in the event of a chargeback. It will be our responsibility to ensure that the correct IAV (CAVV, AAV) ECI, and XID (for Visa) value is attached to both the authorisation and/or settlement transaction. This information will not be made available to you.

We may ask you to provide transaction information to support a card issuer Retrieval Request (RFI – see section 7.5). If you do not provide the requested information you may risk losing the liability shift afforded by Internet Authentication.

2.4 Card Issuer In-line Window

If a cardholder is registered with their issuer, they will see a browser in-line window, which will allow them to enter their password for authentication. We maintain control of the in-line window. This ensures a consistent service to your customers and allows us to monitor the window in case of time out or corrupt data.

2.5 Your Authentication Merchant Information

We will allocate you specific data to participate in the service, and will register this with each scheme. This will allow you to process authentication transactions through each scheme. There is no integration required by you.

2.6 Message Values

Cardholder Authentication generates new message values to indicate the level of security employed, plus the result of the authentication. We will ensure the ePDQ HPP processes all new message values correctly. There may be occasions where authentication is not possible (e.g. in-line window does not appear). You must decide if you wish to continue processing the transaction. This is configurable by you on the ePDQ HPP. Full instructions will be provided in the ePDQ HPP integration guide.

2.7 BIN Cache

The BIN Cache is a repository of BIN ranges held locally (on the Hosted Authentication service server) that are participating in the authentication scheme. Each authentication request will first check the BIN Cache to see if the issuer is participating. If the issuer is not listed in the BIN Cache then you are able to claim an 'attempted authentication'. If the issuer is listed, the HPP will continue to try to obtain authentication. We will update the BIN Cache every 24 hours and check each transaction on your behalf.

2.8 Use of the Verified by Visa and SecureCode™ Logos

The ePDQ HPP displays the Verified by Visa and SecureCode™ logos on each page. This will provide your customers with the assurance that you are participating in the scheme(s) and have been fully registered to participate. If at any stage you request not to use the Authentication service, we will remove both logos from the ePDQ HPP. Both card schemes require the logos to be displayed as evidence of participation in the service.

Section 3 – Hosted Service Users

If you have chosen to authenticate cardholders by connecting to our Hosted Authentication service you must be aware of your responsibilities, as the success of authentication processing relies on your ability to integrate and communicate effectively with us.

We will provide you with the means to communicate with the Hosted Authentication service.

3.1 Your Responsibilities
You must:

- Sign up for authentication with your chosen payment solution and must specify that you are using the Hosted Authentication solution from Barclaycard Payment Acceptance

- Correctly integrate the Hosted Authentication service according with instructions provided

- Ensure that the authentication responses returned by the Hosted Authentication service are correctly passed to your payment solution for submission in the authorisation message

- Ensure your chosen payment solution (if not ePDQ) is approved by us to process Internet Authentication transactions

- Ensure that the IAV (CAVV for Visa, AAV for SecureCode™) is correctly passed in the authorisation message

- Ensure any additional auxiliary data is passed in the authorisation message

- Ensure any additional data is passed in the clearing message

- Manage the process around the cardholder pop up or in-line window (i.e. size, time outs)

- Manage the process for error scenarios on the pop up or in-line window (i.e. cardholder cancels)

- Secure the Authentication Merchant Information used to register you with the card schemes at all times

- Consider optionally maintaining audit records of authentication transactions.

3.2 Our Responsibilities
We will:

- Register you with each participating card scheme supported by us and signed up by you

- Provide you with the appropriate Authentication Merchant Information as registered with the card schemes

- Provide you with the relevant Hosted Authentication service integration guide

- Process authentication requests submitted from you

- Adhere to relevant card scheme policies

- **Maintain a full audit trail and provide transaction evidence to the card issuer in the event of a chargeback where we believe authentication was correctly performed and where liability shift is available (this does not include RFI – see section 7.5), based on authentication data sent by you**

- **Accept authorisation and clearing messages from your chosen payment solution containing authentication data**

- **Provide software upgrades where required (i.e. to support a new card scheme) and upgrade documentation.**

3.3 Transaction Records

We will maintain authentication transaction records on your behalf and will use these to provide evidence that the transaction was authenticated in the event of a chargeback. It will be your responsibility to ensure that the correct IAV (CAVV, AAV) and ECI value is attached to both the authorisation and settlement transaction.

As you control the submission of authentication requests through the Hosted Authentication service you are responsible for ensuring correct integration. Whilst we will defend a chargeback based on the information held on our systems, our records will be based on information received from you. If the card issuer continues to dispute the validity of the authentication we may ask you to provide additional audit evidence as shown in the table on the next page. If you are unable to supply this, the transaction may be charged back to you.

Full Authentication (Visa) Full UCAF (MasterCard and Maestro)	ECI value = 5 CAVV Supplied in human readable format PAReq/PARes XID	ECI value = 2 AAV Supplied in human readable format PAReq/PARes
Attempted Authentication (Visa) Merchant UCAF (MasterCard and Maestro)	ECI value = 6 Attempts CAVV Supplied in human readable format	ECI value = 1 AAV (if supplied) VEReq/VERes OR PAReq/PARes

We may ask you to provide transaction information to support a card issuer Retrieval Request (RFI – see section 7.5). If you do not provide the requested information you may risk losing the liability shift afforded by Internet Authentication.

3.4 Card Issuer Pop Up or In-line Window

It is strongly recommended that you use an in-line window to prevent problems commonly associated with pop up suppression (also referred to as pop up killers) and avoid situations where customers inadvertently close the pop up window. Whether you use pop up or in-line, it is your responsibility to present the browser pop up or in-line window to the cardholder. The card issuer will populate the content and will perform the authentication. You must control the size, time out and error handling conditions associated with the window.

The recommended size of the pop up or in-line window will be provided in the integration documentation. If you choose to support an in-line window you must do so in accordance with the guidelines provided.

It is recommended that the time out for the pop up or in-line window is set to a reasonable time to allow cardholders sufficient time to authenticate themselves. It is your responsibility to set this in line with your website and risk policy. You must ensure you display an adequate error message to the cardholder should you enforce your time out.

There may be occasions where the cardholder closes, cancels or cannot view the pop up or in-line window. You must ensure your website is capable of handling the error responses associated with this and must display clear error messages to the cardholders. It is recommended that you should maintain a balance of informative and non-specific information so as not to assist potential fraud.

3.5 Your Authentication Merchant Information

We will allocate you specific data to participate in the service, and will register this with each scheme. This will allow you to process Authentication transactions through each scheme.

You will need to code these details into your integration with the Hosted Authentication service and pass them on each authentication request. You must ensure that you correctly integrate the information we provide which may be different for each scheme.

Failure to pass the correct details could result in a failure of authentication request.

Once integrated, you should not amend this information unless advised by us. If you lose this information or feel it has been compromised in any way you should contact us immediately. We will issue you with new details and re-register you with the relevant card scheme(s). This process may take up to 10 working days.

3.6 Message Values

Cardholder authentication generates new message values to indicate the level of security employed, plus the result of the authentication.
The Hosted Authentication service will return responses and message values that must be correctly mapped to your chosen payment solution.

The key value is the Issuer Authentication Value (IAV). For Visa, this will be the CAVV and for MasterCard, this will be the AAV. The IAV will always be provided by the card issuer and should not be altered. Your payment solution will also need to ensure the correct eCommerce indicator (ECI) is attached to the authorisation and clearing message.

The table below provides a definition of the ECI values used by each card scheme:

Visa:

5	Authentication is successful.
6	Authentication is attempted but cardholder was not registered.
7	Authentication is unsuccessful or not attempted (standard eCommerce transaction).

MasterCard and Maestro:

2	Authentication is successful. Full UCAF.
1	Authentication is attempted but cardholder was not registered. Merchant UCAF.
0	Authentication is unsuccessful or not attempted (standard eCommerce transaction).

The integration guide we will supply will provide details on how you should correctly map authentication values into your chosen payment solution.

You must ensure your payment solution supports the required level of APACS to communicate with our acquiring system. You can obtain this information by contacting us. You are not required to do this if you use the ePDQ service.

3.7 BIN Cache

The BIN Cache is a repository of BIN ranges held locally (on the Hosted Authentication service server) that are participating in the authentication scheme. You can check the BIN Cache before contacting the relevant scheme Directory to check whether a cardholder is participating. This could reduce the number of messages you are required to generate. We will update the BIN Cache every 24 hours.

3.8 Use of the Verified by Visa and MasterCard Logos

Following successful registration and integration of the authentication software you must download and display the Verified by Visa and MasterCard SecureCode™ logos on your website payment page. These logos will demonstrate to your customers that you are participating in each of the schemes.

The logos will be available from a specific URL (web address) which will be made available to you upon successful application. Instructions will be provided to enable you to download and display the logo.

Section 4 – Barclaycard SmartPay Hosted Payment Page Users

You must read this section if you are using the Barclaycard SmartPay Hosted Payment Page with integrated cardholder authentication.

The Barclaycard SmartPay Hosted Service is a fully hosted payment and authentication service. If you use the Barclaycard SmartPay Hosted Payment Page you will not have to integrate any additional software for cardholder authentication. Once you have successfully applied for the service we will activate the Barclaycard SmartPay Hosted Payment Page to perform authentication on all relevant transactions.

Although the Barclaycard SmartPay Hosted Payment Page requires no specific authentication integration, you must ensure that you have correctly installed the Barclaycard SmartPay Hosted Payment Page in line with the instructions provided to you. Failure to do this may result in incorrect transaction processing.

4.1 Your Responsibilities
We control the authentication process within the Barclaycard SmartPay Hosted Payment Page and will ensure you have minimal disruption to your current transaction processing. You must:

- Correctly integrate the Barclaycard SmartPay Hosted Payment Page in line with instructions provided at sign up

- Read and understand how the Barclaycard SmartPay Hosted Payment Page handles authenticated transactions – this information is provided in the integration guides

- Request Activation of the Barclaycard SmartPay Hosted Payment Page

- Advise us immediately if you cease using the Barclaycard SmartPay Hosted Payment Page.

4.2 Our Responsibilities
We will:

- Register you with each participating card scheme supported by us

- Provide you with the Barclaycard SmartPay integration guide

- Configure Barclaycard SmartPay to allow your transaction process to authenticate transactions

- Control the processing of authentication transactions

- Adhere to relevant card scheme policies

- Process transactions accordingly for "failure" scenarios in line with your configuration requirements for Barclaycard SmartPay

- Maintain a full audit trail and provide transaction evidence to the card issuer in the event of a chargeback where we believe authentication was correctly performed and where liability shift is available (this does not include Retrieval Requests (RFI) – see section 7.5)

- Ensure the correct authentication values are attached to both the authorisation and clearing message where appropriate.

4.3 Transaction Records

We will maintain authentication transaction records on your behalf and will use these to provide evidence that the transaction was authenticated in the event of a chargeback. It will be our responsibility o ensure that the correct IAV (CAVV, AAV) ECI, and XID (for Visa) value is attached to both the authorisation and/or settlement transaction. This information will not be made available to you.

We may ask you to provide transaction information to support a card issuer Retrieval Request (RFI – see section 7.5). If you do not provide the requested information you may risk losing the liability shift afforded by Internet Authentication.

4.4 Card Issuer In-line Window

If a cardholder is registered with their issuer, they will see a browser in-line window, which will allow them to enter their password for authentication. We maintain control of the in-line window. This ensures a consistent service to your customers and allows us to monitor the window in case of time out or corrupt data.

4.5 Your Authentication Merchant Information

We will allocate you specific data to participate in the service, and will register this with each scheme. This will allow you to process authentication transactions through each scheme. There is no integration required by you.

4.6 Message Values

Cardholder Authentication generates new message values to indicate the level of security employed, plus the result of the authentication. We will ensure the Barclaycard SmartPay Hosted Payment Page processes all new message values correctly. There may be occasions where authentication is not possible (e.g. in-line window does not appear or a time out).

In the event that a participating cardholder cannot authenticate themselves, a Visa transaction must be declined. If this occurs, depending on the issuer, Barclaycard SmartPay will decline the transaction.

Please note: MasterCard and Maestro transactions are permitted to continue. See section 7 for more information.

4.7 BIN Cache

The BIN Cache is a repository of BIN ranges held with the schemes Directory service and contains the details of the participating issuer in the authentication scheme. Each authentication request will first check the BIN Cache to see if the issuer is participating. If the issuer is not listed in the BIN Cache then you are able to claim an 'attempted authentication'. If the issuer is listed, Barclaycard SmartPay will continue to try and obtain authentication.

4.8 Use of the Verified by Visa and SecureCode™ Logos

You are able to display the Verified by Visa and SecureCode™ logos on the Barclaycard SmartPay Hosted Payment page. This will provide your customers with the assurance that you are participating in the scheme(s) and have been fully registered to participate. If at any stage you request not to use the Authentication service, you will need to remove both logos from your payment page and skin template. Both card schemes require the logos to be displayed as evidence of participation in the service.

Section 5 – Barclaycard SmartPay API Service Users

You must read this section if you are using the Barclaycard SmartPay API Service with integrated cardholder authentication.

If you use the Barclaycard SmartPay API Service you will not have to integrate any additional software for cardholder authentication. However, you must ensure that:

1. Your processing account has been configured by Barclaycard SmartPay to support Internet Authentication

2. Your software supports redirecting the shopper to the card issuer and submitting a second API call to complete the payment.

Once you have successfully applied for the service we will activate he Barclaycard SmartPay API Service to perform authentication on all relevant transactions.

Although the Barclaycard SmartPay API Service requires no specific authentication integration, you must ensure that you have correctly installed the Barclaycard SmartPay API in line with the instructions provided to you. Failure to do this may result in incorrect transaction processing.

5.1 Your Responsibilities
We control the authentication process within the Barclaycard SmartPay API and will ensure you have minimal disruption to your current transaction processing. You must:

• Correctly integrate the Barclaycard SmartPay API Service in line with instructions provided at sign up

• Read and understand how the Barclaycard SmartPay API Service handles authenticated transactions – this information is provided in the integration guides

• Request Activation of the Barclaycard SmartPay API Service

• Advise us immediately if you cease using the Barclaycard SmartPay API Service.

5.2 Our Responsibilities
We will:

• Register you with each participating card scheme supported by us

• Provide you with the Barclaycard SmartPay integration guide

• Configure Barclaycard SmartPay to allow your transaction process to authenticate transactions

• Control the processing of authentication transactions

• Adhere to relevant card scheme policies

• Process transactions accordingly for "failure" scenarios in line with your configuration requirements for Barclaycard SmartPay

• Maintain a full audit trail and provide transaction evidence to the card issuer in the event of a chargeback where we believe authentication was correctly performed and where liability shift is available (this does not include Retrieval Requests (RFI) – see section 7.5)

• Ensure the correct authentication values are attached to both the authorisation and clearing message where appropriate.

5.3 Transaction Records

We will maintain authentication transaction records on your behalf and will use these to provide evidence that the transaction was authenticated in the event of a chargeback. It will be our responsibility to ensure that the correct IAV (CAVV, AAV) ECI, and XID (for Visa) value is attached to both the authorisation and/or settlement transaction. This information will not be made available to you.

We may ask you to provide transaction information to support a card issuer Retrieval Request (RFI – see section 7.5). If you do not provide the requested information you may risk losing the liability shift afforded by Internet Authentication.

5.4 Card Issuer In-line Window

If a cardholder is registered with their issuer, they will see a browser in-line window, which will allow them to enter their password for authentication. We maintain control of the in-line window. This ensures a consistent service to your customers and allows us to monitor the window in case of time out or corrupt data.

5.5 Your Authentication Merchant Information

We will allocate you specific data to participate in the service, and will register this with each scheme. This will allow you to process authentication transactions through each scheme.

5.6 Message Values

Cardholder Authentication generates new message values to indicate the level of security employed, plus the result of the authentication. We will ensure the Barclaycard SmartPay API Service processes all new message values correctly. There may be occasions where authentication is not possible (e.g. in-line window does not appear or a time-out).

In the event that a participating cardholder cannot authenticate themselves, a Visa transaction must be declined. If this occurs, depending on the issuer, Barclaycard SmartPay will decline the transaction.

Please note: MasterCard and Maestro transactions are permitted to continue. See section 7 for more information.

5.7 BIN Cache

The BIN Cache is a repository of BIN ranges held with the schemes Directory service and contains the details of the participating issuer in the authentication scheme. Each authentication request will first check the BIN Cache to see if the issuer is participating. If the issuer is not listed in the BIN Cache then you are able to claim an 'attempted authentication'. If the issuer is listed, Barclaycard SmartPay will continue to try and return a URL supplied by the issuer for you to display to the shopper.

5.8 Use of the Verified by Visa and SecureCode™ Logos

You are able to display the Verified by Visa and SecureCode™ logos on the Barclaycard SmartPay Payment page. This will provide your customers with the assurance that you are participating in the scheme(s) and have been fully registered to participate. If at any stage you request not to use the Authentication service, we will remove both logos from Barclaycard SmartPay. Both card schemes require the logos to be displayed as evidence of participation in the service.

Section 6 – Direct to Card Schemes

If you have chosen to source or build your own authentication solution that communicates directly with the participating card schemes you are responsible for the whole authentication process and must ensure strict adherence to the integration and implementation requirements.

If you are using a third party product to support Internet Authentication you must ensure that they can support the requirements detailed in this section.

6.1 Your Responsibilities
You must:

- Sign up for authentication, providing details of your chosen payment solution and must specify that you only wish to be registered for the service

- Ensure your chosen payment solution (if not ePDQ) is approved by us to process Internet Authentication transactions

- Correctly build and implement your authentication and payment solution in line with the latest 3D Secure Protocol and APACS standards

- Obtain full type approval from us to use the APACS standards at the required level

- Ensure that the authentication responses returned by your authentication solution are correctly passed to your payment solution for submission in the authorisation message

- Ensure that the IAV (CAVV for Visa, AAV for SecureCode™) is correctly passed in the authorisation message

- Ensure any additional auxiliary data is passed in the authorisation message

- Ensure any additional data is passed in the clearing message

- Manage the process around the cardholder pop up or in-line window (i.e. size, time outs)

- Manage the process for error scenarios on the pop up or in-line window (i.e. cardholder cancels)

- Secure the Authentication Merchant Information used to register you with the card schemes at all times

- Ensure the BIN Cache for each scheme (if being used) is updated at least every 24 hours

- Maintain FULL audit records of authentication transactions (including BIN Cache updates)

- Provide us with evidence of authentication should we require this to defend a chargeback. This information must be returned to us within 14 days of our original request.

6.2 Our Responsibilities

We will:

- Register you with each participating card scheme supported by us and signed up to by you

- Provide you with the appropriate Authentication Merchant Information as registered with the card schemes

- Accept authorisation and clearing messages from your chosen payment solution containing authentication data

- Provide transaction evidence to the card issuer in the event of a chargeback where we believe authentication was correctly performed and where liability shift is available based on information received from you

- Provide scheme or protocol updates to you when applicable.

6.3 Transaction Records

You must maintain and store full authentication records to provide evidence should an authenticated transaction be charged back.
The table on the next page shows what evidence will be required in the event of a disputed transaction:

Full Authentication (Visa) Full UCAF (MasterCard and Maestro)	ECI value = 5 CAVV Supplied in human readable format PAReq/PARes XID	ECI value = 2 AAV Supplied in human readable format PAReq/PARes
Attempted Authentication (Visa) Merchant UCAF (MasterCard and Maestro)	ECI value = 6 Attempts CAVV Supplied in human readable format	ECI value = 1 AAV (if supplied) VEReq/VERes OR PAReq/PARes

Note: If your solution supports BIN Cache, you must also supply CRReq/CRRes.

We may ask you to provide transaction information to support a card issuer Retrieval Request (RFI – see section 7.5). If you do not provide the requested information you may risk losing the liability shift afforded by Internet Authentication.

6.4 Card Issuer Pop Up or In-line Window

It is your responsibility to present the browser pop up or in-line window to the cardholder. The card issuer will populate the content and will perform the authentication. You must control the size, time out and error handling conditions associated with the window.

It is strongly recommended that you use an in-line window to prevent problems commonly associated with pop up suppression (also referred to as pop up killers) and avoid situations where customers inadvertently close the pop up window. Whether you use pop up or in-line, it is your

responsibility to present the browser pop up or in-line window to the cardholder. The card issuer will populate the content and will perform the authentication. You must control the size, time out and error handling conditions associated with the window.

Your authentication software supplier should provide the recommended size of the pop up or in-line window.

It is recommended that the time out for the pop up or in-line window is set to a reasonable time to allow cardholders sufficient time to authenticate themselves. It is your responsibility to set this in line with your website and risk policy. You must ensure you display an adequate error message to the cardholder should you enforce your time out.

There may be occasions where the cardholder closes cancels or cannot view the pop up or in-line window. You must ensure your website is capable of handling the error responses associated with this and must display clear error messages to the cardholders. It is recommended that you should maintain a balance of informative and non-specific information so as not to assist potential fraud.

6.5 Your Authentication Merchant Information

We will allocate you specific data to participate in the service, and will register this with each scheme. This will allow you to process authentication transactions through each scheme.

You will need to code these details into your authentication solution and pass them on each authentication request. You must ensure that you correctly integrate the information we provide which may be different for each scheme. Failure to pass the correct details could result in a failure of authentication request.

Once integrated, you should not amend this information unless advised by us. If you lose this information or feel it has been compromised in any way you should contact us immediately. We will issue you with new details and re-register you with the relevant card scheme(s). This process may take up to 10 working days.

Please note that this information will not be supplied to any third party payment provider acting on your behalf. It will only be provided directly to you.

6.6 Message Values

Cardholder authentication generates new message values to indicate the level of security employed, plus the result of the authentication. You must ensure that you fully understand the responses sent to your authentication solution by the card schemes and pass this to your payment solution in the authorisation and clearing messages.

The key value is the Issuer Authentication Value (IAV). For Visa, this will be the CAVV and for MasterCard, this will be the AAV. The IAV will always be provided by the card issuer and should not be altered. Your payment solution will also need to ensure the correct eCommerce indicator (ECI) is attached to the authorisation and clearing message.

The table on the next page provides a definition of the ECI values used by each card scheme:

Visa:

5	Authentication is successful.
6	Authentication is attempted but cardholder was not registered.
7	Authentication is unsuccessful or not attempted (standard eCommerce transaction).

MasterCard and Maestro:

2	Authentication is successful. Full UCAF.
1	Authentication is attempted but cardholder was not registered. Merchant UCAF.
0	Authentication is unsuccessful or not attempted (standard eCommerce transaction).

Your authentication software integration guide will provide details on how you should correctly map authentication values into your chosen payment solution.

You must ensure your payment solution supports the required level of APACS to communicate with our acquiring system. You can obtain this information by contacting us.

6.7 BIN Cache

The BIN Cache is a repository of BIN ranges that can be held locally on your server. If you wish to use the BIN Cache you must contact each scheme directory using the appropriate 3D Secure requests (CRReq/CRRes) to download the latest version at least every 24 hours. You can check the BIN Cache before contacting the relevant scheme Directory to check whether a cardholder is participating. This could reduce the number of messages you are required to generate.

Please note: Visa are currently assessing whether the BIN Cache is still required and will consider removing it once adoption has increased.

6.8 Use of the Verified by Visa and SecureCode™ Logos

Following successful registration and integration of the authentication software you must download and display the Verified by Visa and SecureCode™ logo on your web site payment page. These logos will demonstrate to your customers that you are participating in each of the schemes.

The logos will be available from a specific URL (web address) which will be made available to you upon successful application. Instructions will be provided to enable you to download and display the logo.

Section 7 – Card Scheme Compliance

The following section provides information required by the card schemes participating in cardholder authentication. It is important to understand any responsibilities you may have. This will vary according to which payment product you use.

7.1 Protocol Support
You must support the 3D Secure Protocol v1.0.2 or above.
The following products adhere to this standard:

- **The ePDQ HPP**
- **The ePDQ API**
- **Barclaycard SmartPay Hosted Payment Page**
- **Barclaycard SmartPay API**
- **Hosted Authentication service.**

If you are using any other product you must ensure your solution meets this requirement.

7.2 Authentication Failure
Typically, if a cardholder is registered for authentication they will be familiar with the process to correctly authenticate themselves. There may, however, be occasions where the cardholder does not follow the correct process, or where a card may be being used fraudulently. The following scenarios may occur:

1. **The cardholder may fail to key in their correct password (maximum of three attempts), or**

2. **The cardholder may cancel the pop up or in-line window, or**

3. **The cardholder may close the pop up or in-line window, or**

4. **The pop up or in-line window may time out, or**

5. **The content of the window may be corrupt due to issuer error**

6. **The cardholder browser may suppress the pop-up.**

The above scenarios (page 47) can be described as:

Failed Authentication (scenario 1)

Error during Authentication (scenarios 2-6).

Each of the card schemes have set policies to handle the above:

Visa:

If authentication fails (scenario 1) you will receive an 'N' response within the PARes message. You must decline the transaction and stop further processing, because the cardholder could not authenticate themselves.

The ePDQ HPP and Barclaycard SmartPay Hosted Payment Pages will do this automatically.

In scenarios 2, 3, 4, 5 and 6 you may choose to proceed with the transaction and must be aware that you will **lose the protection** afforded by the chargeback liability shift (i.e. you could still be charged back).

The ePDQ HPP will either decline or continue with the transaction based on how you set up the appropriate continuity flags within the ePDQ technical settings.

Barclaycard SmartPay Hosted Payment Page will automatically either decline or continue the transaction based on the response returned by the issuer and inline with scheme rules.

MasterCard and Maestro:

If authentication fails (scenario 1) you will receive an 'N' response within the PARes message. You have the option of either:

Declining the transaction and stop further processing, because the cardholder could not authenticate themselves,

Or,

Progressing and attempting authorisation.

If you do proceed and are given an authorisation code by the card issuer, you will not benefit from liability shift. If authorisation is not given, the card must be declined in the normal way.

In scenarios 2, 3, 4, 5 and 6 you may choose to proceed with the transaction and must be aware that you will **lose the protection** afforded by the chargeback liability shift (i.e. you could still be charged back).

Barclaycard SmartPay Hosted Payment Page will automatically either decline or continue the transaction based on the response returned by the issuer and inline with scheme rules.

7.3 Passing Authentication Values

As detailed above, you must ensure compliance with 3D Secure Protocol v1.0.2. You will also need to ensure that you can pass the authentication results in your authorisation and clearing message. You must have integrated the APACS standard that supports this. Information on which standard is used can be obtained by contacting us. If you use ePDQ or Barclaycard SmartPay you do not have to do this.

You must be capable of receiving and passing:

- **Issuer Authentication Value (IAV) – CAVV for Visa, AAV for SecureCode™**

- **ECI values**

- **XID (for Visa)**

- **3D Secure Protocol messages.**

It is your responsibility to ensure that the values, if received from the card issuer are not altered in any way and are passed as received. The CAVV or AAV could be incorrectly passed if:

- **The payment solution you are using does not support these values.**

- **There is a problem with your integration to the Hosted Authentication service and/or payment software.**

An incorrect ECI value could be passed if:

- **There is a problem with your integration to the Hosted Authentication service and/or payment software.**

- **You have registered to participate but have not advised us you wish to go live**

- **You have inadvertently hard coded every ECI value to a set parameter (i.e. ECI 7 for standard eCommerce).**

You must make every attempt to avoid the possible errors above. In the event that you fail to pass the IAV, or incorrectly pass the ECI value, you will not benefit from liability shift under any circumstances. In the event that you purposefully falsify any authentication value we may end your authentication and merchant agreements.

Only ePDQ HPP and Barclaycard SmartPay Hosted Payment Page will automatically control the processing of authentication values. Please be aware that the ECI values passed must match for both the authorisation and the clearing message.

7.4 Error Conditions

In the unlikely event that you experience an error condition whilst using cardholder authentication, you need to ensure you can handle the responses.

Scheme Directory Server Unavailable

You may see an error where the HPP, Barclaycard SmartPay, or your own solution cannot connect to the relevant scheme directory.
If this is the case, you will be sent a corresponding error message, which must be interpreted and handled appropriately.

If the directory server is unavailable, this is considered a "break" in the authentication process as neither a positive (success) or negative (failure) message can be supplied. As such, different liability shift rules apply:

Visa:

You can continue with the transaction, but must pass an ECI 7 as this was a non-authenticated transaction. You **will not** benefit from any chargeback protection.

For MasterCard and Maestro:

If you have correctly integrated the HPP, Barclaycard SmartPay or your own solution and get this error, you can claim Merchant UCAF and still receive liability shift (subject to the conditions in 1.4). The ePDQ HPP will process transactions based on your settings within the ePDQ technical setting. Barclaycard SmartPay Hosted Payment Page will process the transaction based on the response returned by the issuer and inline with scheme rules.

Hosted Authentication service Unavailable

If you are unable to authenticate transactions because Hosted Authentication service is not operating, this is also perceived as a "break" in the process but has a different outcome.

If the Hosted Authentication service is unavailable you should report this to us immediately. Transactions will not be authenticated if this service is down. You can continue with the transaction, but must pass an ECI 7 for Visa or ECI 0 for MasterCard as this was a non-authenticated transaction. You **will not** benefit from any chargeback protection for either card scheme.

If the ePDQ HPP detects that the Hosted Authentication service is down it will process transactions based on your configuration of the ePDQ technical settings.

With Barclaycard SmartPay if the Hosted Authentication service is down then transactions will be unable to continue for authorisation.

Cardholder Browser Suppresses Pop Up Window

If the cardholder browser does not allow the pop up to be displayed, this is also considered as a "break" in the authentication request. As with the scenarios above, you may continue with the transaction but for Visa transactions you will not benefit from any chargeback protection. As recommended, you should consider the use of an in line window to avoid such errors.

Own Authentication Software Unavailable

The same conditions as above apply.

7.5 Retrievals (Requests for Information – RFI)

You may, on occasion receive an RFI from us asking for specific transaction information. RFIs are generated by the card issuers and must be passed to you. The card issuers, under card scheme rules, are not obliged to advise why they require information on the transaction nor are they obliged to provide the cardholder name.

If we receive an RFI for a transaction you have processed we will send you a letter asking you to provide specific transaction information. This information relates to the details of the transaction and does not relate to the level or result of authentication used. An RFI may be sent to you regardless of which product(s) you are using for cardholder authentication and payment processing.

A card issuer may issue an RFI for various reasons. The most common examples are below:

- **The Cardholder is denying the transaction, even though it was authenticated. The Card Issuer will require details of the transaction (e.g. to see if delivery was to the billing address) for any legal/recovery action that they may be taking against their Cardholder**

- **The Cardholder requires details of the transaction for their own records (e.g. to assist in a company expense claim such as a flight bought for company travel)**

- **The Card Issuer/Cardholder requires details of the transaction because they are in dispute with the you e.g. the goods are faulty or they have been charged a different amount and they want to know what for**

- **The transaction was a T&E transaction and there is a dispute e.g. the Card Issuer/Cardholder requires details of a Car Hire Agreement, Hotel Cancellation Policy etc**

- **You will have 14 days to reply to the RFI supplying the information requested. If this information is not received and returned to the card issuer in time, you will forfeit any protection that cardholder authentication offers.**

If you receive an RFI, we will provide a template reply letter, which must be returned on your business headed paper. An example of some of the information requested is provided below:

Case Id:

Your Web site Address:

Card Holder Name:

Card Number:

Expiry Date:

Amount:

Nature of Goods/Service:

Transaction Date:

Authorisation Code:

Date And Amount Of Refund (If Applicable).

It is important you understand the impact that failure to respond to an RFI may have on any chargeback liability shift. If you have any questions please contact us.

Appendix A – Liability Shift Rules

Liability Shift Cover for Visa Card

Card Type	Authentication	CAVV	ECI	Description	Liability Shift?
Standard Card – EU Region	Obtained	Yes	5	Authentication successful by cardholder. Issuer generated CAVV	Yes
	Attempted	Optional	6	Authentication attempted but cardholder not enrolled. Issuer optionally generates CAVV. If received CAVV must be passed in the authorisation message	Yes
	Unsuccessful	No	7	Authentication failed or not attempted	No

Card Type	Authentication	CAVV	ECI	Description	Liability Shift?
Standard Card – Rest of the World	Obtained	Yes	5	Authentication successful by cardholder. Issuer generated CAVV	Yes
	Attempted	Optional	6	Authentication attempted but cardholder not enrolled. Issuer optionally generates CAVV. If received CAVV must be passed in the authorisation message	Yes
	Unsuccessful	No	7	Authentication failed or not attempted	No

Card Type	Authentication	CAVV	ECI	Description	Liability Shift?
Commercial Card – EU Region	Obtained	Yes	5	Authentication successful by cardholder. Issuer generated CAVV	Yes
	Attempted	Optional	6	Authentication attempted but cardholder not enrolled. Issuer optionally generates CAVV. If received CAVV must be passed in the authorisation message	Yes
	Unsuccessful	No	7	Authentication failed or not attempted	No

Card Type	Authentication	CAVV	ECI	Description	Liability Shift?
Commercial card [1] – Rest of the World	Obtained	Yes	5	Authentication successful by cardholder. Issuer generated CAVV	Yes
	Attempted	Optional	6	Authentication attempted but cardholder not enrolled. Issuer optionally generates CAVV. If received CAVV must be passed in the authorisation message	Yes
	Unsuccessful	No	7	Authentication failed or not attempted	No

In the event that the Visa card issuer does not return a CAVV for an attempted authentication, you can still claim liability shift using an ECI 6. However, liability shift is only available for European region issued cards in this scenario. Full Rest of the World liability is only provided if the card issuer supplies a CAVV.

[1] Excluded cards are detailed in section 1.7.

Liability Shift Cover for MasterCard

As liability shift on MasterCard can be influenced by the result of the authorisation request, an additional column has been added to this table to indicate both the authentication and authorisation position.

Card Type	Authentication	AAV	ECI	Description	Authorised?	Liability Shift?
All Cards – European Region	Obtained	Yes	2	Authentication successful by cardholder. Issuer generated AVV. Full UCAF	Yes	Yes
All Cards[1] – European Region	Attempted	Yes	1	Authentication attempted but cardholder not enrolled. Issuer may generate AAV. Merchant UCAF	Yes	Yes
	Unsuccessful	No	1	Authentication failed	Yes. If not authorised: No	No

Card Type	Authentication	AAV	ECI	Description	Authorised?	Liability Shift?
All Cards – Rest of the World	Obtained	Yes	2	Authentication successful by cardholder. Issuer generated AVV. Full UCAF	Yes	Yes
All Cards[1] – European Region	Attempted	Yes	1	Authentication attempted but cardholder not enrolled. Issuer may generate AAV. Merchant UCAF	Yes	Yes
	Unsuccessful	No	1	Authentication failed	Yes If not authorised: No	No

In the event that the MasterCard card issuer does not return an AAV for an attempted authentication, you can still claim liability under Merchant UCAF as long as you meet the conditions described in this procedure guide.

[1] Excluded cards are detailed in section 1.7.

Liability Shift Cover for Maestro

As liability shift on Maestro can be influenced by the result of the authorisation request, an additional column has been added to this table to indicate both the authentication and authorisation position.

Card Type	Authentication	AAV	ECI	Description	Authorised?	Liability Shift?
Cards issued in the UK only	Obtained	Yes	2	Authentication successful by cardholder. Issuer generated AVV. Full UCAF	Yes	Yes
	Attempted	Yes	1	Authentication attempted but cardholder not enrolled. Issuer may generate AAV. Merchant UCAF	Yes	Yes
	Unsuccessful	No	1	Authentication failed	Yes If not authorised: No	No

Card Type	Authentication	AAV	ECI	Description	Authorised?	Liability Shift?
Cards issued outside the UK only	Obtained	Yes	2	Authentication successful by cardholder. Issuer generated AVV. Full UCAF	Yes	Yes
	Attempted	Yes	1	Authentication attempted but cardholder not enrolled. Issuer may generate AAV. Merchant UCAF	Yes	Yes
	Unsuccessful	No	1	Authentication failed	Yes If not authorised: No	No

In the event that the UK Maestro card issuer does not return an AAV for an attempted authentication, you can still claim liability under Merchant UCAF as long as you meet the conditions described in this procedure guide.

Appendix B – Managing Internet Fraud 'Best Practice'

In the physical, traditional retailing world, where the cardholder and card are both present at the point of sale, merchants can adopt measures to confirm that the genuine cardholder is making the purchase. These include:

- Talking to Authorisations if suspicious
- Checking the card signature on the card with the signature on the receipt
- Chip & PIN utitlisation
- Name awareness – i.e. Mr P Smith embossed on the card being presented by a female
- Other forms of identification may be requested.

Taking card payments over the internet means that none of these checks can be carried out at the time of the transaction, because the process is fully automated and therefore no manual intervention can take place. However, you will have collected information about the customer and their purchase on the order and payment pages of your website, which will help you to take measures to reduce the threat of chargebacks and stolen goods.

There are some simple questions you can ask yourself about customer not present orders:

- Is the sale too easy? Is the customer uninterested in the price or details of the goods?
- Are they a new customer?

- Are the goods high value or easily resalable?
- Is the sale excessively high in comparison with your usual orders? Is the customer ordering many different items? Do they seem unlike your usual customer?
- Is the customer providing details of someone else's card e.g. that of a client or a family member?
- Is the customer reluctant to give a landline contact phone number – are they only prepared to give a mobile number?
- Does the address provided seem suspicious? Has the delivery address been used before with different customer details?
- Is the customer being prompted by a third party whilst on the phone (if a telephone order)?
- Is the customer attempting to use more than one card in order to split the value of the sale?
- Does the customer seem to lack knowledge of their account?
- Does the customer seem to have a problem remembering their home address or phone number? Does the customer sound as if they are referring to notes?
- Have they used a free email address such as @hotmail.com or an email forwarding address?
- Does the email address match the name of the cardholder?
- Has their email bounced?

There are a number of tools that you can use to verify these questions, for example, Internet Authentication, Address Verification Service and Card Security Code checking service.

Internet Authentication – is an industry-wide initiative to fight fraud and protect businesses trading over the internet. It allows Visa card and MasterCard issuers to request their cardholders buying from your website to enter a password online. This will automatically verify their identity and authenticate the card, so you can accept their payment with confidence.

Address Verification Service – checks the details supplied for the cardholder's billing address and postcode against that held on the card issuers records by checking the postcode and address numbers, for example:

1234 Pavilion Drive
Northampton
NN4 7SG

The numbers entered 1234 and 47 are checked by the card issuer who confirm if the details match or not.

Card Security Code checking – this service works by checking that the unique 3 digit code on the rear of most cards, and 4 digit code on the front of American Express cards match the details held by the card Issuer.

Internet Authentication, Address Verification Service and Card Security Code Checking are all available from Barclaycard Payment Acceptance. They are available as part of our on-line payment solution ePDQ.

ePDQ provides a very comprehensive Risk Management module. This provides standard rules, lists and default checks that can be used to try and identify and alert you to potentially fraudulent transactions.

Risk Management systems, such as that offered by ePDQ, can help you to recognise and hopefully remove fraudulent transactions from being processed through your business.

No Risk Management system can definitively determine whether any given transaction is, in fact, fraudulent. Therefore, fraud protection systems can form only one part of a comprehensive business decision-making process that involves human oversight and investigation of each transaction in question.

www.bt.com/phonenetuk/ offers a service where you can check the billing/delivery address against the telephone number.

In addition, various other organisations provide services that allow you to check name, address and postcode details.

www.equifax.co.uk	Provides a service to check details against the electoral register.
www.royalmail.com	Provides a service to check the address against postcode and vice versa.
www.streetmap.co.uk	Provides a facility to input a postcode and view the address details.

Note: You may be charged a fee to use all or some of the services provided by the above organisations.

For more information on managing internet fraud, please go to our website at **www.barclaycardbusiness.co.uk** Information Centre, Fraud advice.

This information is available in large print,
Braille or audio format by calling **0800 61 61 61**.*