Business Gateway

Cardholder Authentication Guide

V5.3 May 2016

Use this help to find out:

- How cardholder authentication works
- How liability shift affects you

Contents

1 About this guide

This guide describes cardholder authentication services, and how they work. It also explains liability shift, and how to interpret authentication results.

1.1 Audience

Read this guide if we host your payment pages.

1.2 Changes to the guide

5.3	Corrections and updates to Liability Shift details	May 2016	**What is Liability Shift?**
5.2	Correction to Liability Shift for personal cards table	March 2016	**What is Liability Shift?**
5.1	Update to Liability Shift details	March 2016	**What is Liability Shift?**
5.0	Worldpay rebrand	July 2014	All pages
4.4	Updated Liability Shift details for American Express SafeKey.	February 2014	**What is Liability Shift?**
4.3	Updated Liability Shift details to include a note about V.me	August 2013	**What is Liability Shift?**
4.2	Removed the UK only restriction for Maestro.	March 2013	**What is authentication?**
4.1	Added information about American Express SafeKey.	September 2012	All pages
4.0	Gateway and guide name added to navigation path.	December 2011	All pages
3.1	New cardholder authentication response.	October 2011	**Managing and Interpreting your Authentication Results** **What is Liability Shift?**
3.0	WorldPay rebrand.	July 2011	All pages

1.2.1 Copyright

Worldpay (UK) Limited (Company No: 07316500/ FCA No: 530923), Worldpay Limited (Company No: 03424752 / FCA No: 504504), Worldpay AP Limited (Company No: 5593466 / FCA No: 502597). Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AF and authorised by the Financial Conduct Authority under the Payment Service Regulations 2009 for the provision of payment services. Worldpay (UK) Limited is authorised and regulated by the Financial Conduct Authority for consumer credit activities.

2 What is authentication?

Authentication procedures, along with other fraud protection measures give you a strong anti-fraud strategy that protects your business against criminals.

MasterCard SecureCode, Verified by Visa and American Express SafeKey are 3D secure cardholder authentication schemes that verify a shopper's identity when the shopper buys goods or services online. Knowing the identity of your shoppers helps stop the use of stolen and cloned cards.

If your systems are set up for authentication, the card issuer authenticates the identity of their cardholder when they make an online purchase. Therefore, the liability for any subsequent fraud-related chargeback of that transaction shifts from you to the company that issued the card. This gives you protection against chargebacks due to fraud. For more information, see **What is Liability Shift?**

However, cardholder authentication schemes are applicable to Internet transactions only and do not cover fax, mail, or phone orders. Cardholder authentication is also not available on all card types. For more information, see **Restrictions to Authentication Services**.

Cardholder authentication is mandatory for Maestro. If you want to accept Maestro payments you must be enabled for MasterCard SecureCode.

2.1 Verified by Visa, MasterCard SecureCode and American Express SafeKey

For more about the various cardholder authentication schemes, click the appropriate Web link below, then use the site navigation to locate the appropriate pages:

- **Verified by Visa Europe**
- **Verified by Visa USA**
- **Visa Asia Pacific**
- **MasterCard SecureCode**
- **Maestro**
- **American Express SafeKey**

2.2 How do I use authentication?

In most cases, if you have an existing account, you do not have to make changes to your installation to support authentication. Contact us if you want to enable authentication.

Enfeeblement is effective for all payment methods in a single merchant code. For example, if you enable authentication for Visa, authentication is also enabled for MasterCard in a single merchant code. However, if you want to enable authentication for multiple merchant codes, you must enable authentication individually for each merchant code.

If you do not yet have an account, you can enable authentication services when you apply for an account. If you enable authentication, you will receive the services when we enable your payment pages on our systems. You will then receive authentication details in your transaction results whenever MasterCard, Maestro, Visa and American Express cardholders visit your store.

There are some restrictions to enablement: for example, with Checkout and Invisible merchants, merchants in the USA, and those who use an acquirer other than us. We can advise you on an individual basis when you contact us. See ***Restrictions to Authentication Services****.*

2.3 Authentication - features and benefits

2.3.1 Features

- Authentication page

  Enables your shoppers to confirm their identity with their card issuer
- Authentication results

  Help reassure you as to the identity of the cardholder who made the transaction
- Protection from fraud-related chargebacks

  New rules mean that you may no longer be liable for fraud related chargebacks

2.3.2 Benefits

- Added protection for your business from fraudulent payment attempts
- Allows you to trade online more safely
- Enhances shopper confidence and spending as a result of a more secure e-commerce environment
- Reduces costs from fraud chargebacks (in the majority of cases)

3 How does cardholder authentication work?

When a MasterCard, Maestro, Visa, or American Express cardholder visits your store, the authentication process automatically detects whether the card issuer is participating in authentication and if the cardholder is enrolled for authentication.

When an enrolled cardholder begins the payment process they will be presented with a secure web page, served by their card issuer as part of the payment process. The cardholder must enter their password on this page where it will be sent to their card issuer for comparison.

If the password matches, the cardholder is authenticated and the payment process continues. If the password does not match, payment processing does not continue, preventing potential fraudulent transactions ever reaching you.

This description reflects the process from the viewpoint of a standard merchant account, where our Risk Management service is used. In the case where a merchant supplies their own authentication service and their own risk management, the process may differ, especially if authentication fails.

3.1 Enrolment

Cardholder enrolment is the responsibility of the card issuer. Cardholders can sign-up to MasterCard SecureCode, Verified by Visa and American Express SafeKey via their card issuer.

Enrolment may take a number of forms:

- **Self-enrolment**: The cardholder visits a registration site operated by the card issuer and registers by answering a series of questions, selecting a password and agreeing an assurance message. This provides the cardholder with added confidence that they are communicating with their card issuer during the payment process.
- **Pre-enrolment / Activation During Shopping (ADS)**: Some card issuers pre-enrol their cards for authentication. This results in a cardholder being offered an enrolment page in place of the authentication page when they shop online at a web site which is enabled for authentication.

To facilitate speedy take-up of the service, card issuers are introducing 'Activation During Shopping' (ADS) in the UK as an ideal way to both inform as well as register their cardholders at the time an online transaction is taking place.

To assist these cardholders, issuers enable those who wish to enrol in an authentication programme to do so and allow those who wish to continue with their purchase to by-pass enrolment and proceed to authorisation, as normal. Typically, issuers will limit the number of times a cardholder opts out before forcing enrolment.

3.2 The authentication transaction process

The following steps show what happens when our system authenticates a transaction.

1. The cardholder makes an online purchase with a card.
2. Information is sent to the appropriate card scheme (Visa, Maestro, MasterCard, or American Express) directory server to query whether the card issuer is participating in the relevant scheme.
3. If the card issuer is enroled, the information is sent to the card issuer for them to check if their

cardholder or the card or both are enroled.

4. If the cardholder is enroled, an authentication request is sent to the card issuer by means of the cardholder's browser.
5. The card issuer displays a window that shows their brand name to the cardholder, who is prompted for a password. Note that this information is secure and can be accessed only by the card holder and their card issuer.
6. The card issuer returns the authentication results by means of the cardholder's browser.
7. If an appropriate authentication response is received, the payment is submitted for authorisation, which includes the relevant authentication results.

If the cardholder fails authentication, the card issuer will advise the cardholder to reset their password. In this case, the card holder receives a failed authentication response and the purchase is not submitted for authorisation. The results can be viewed in the Merchant Interface.

3.3 Differences in the payment processes

There are differences in the payment process for cardholder authentication compared with the process without authentication. The following procedures outline the payment process when an enroled cardholder visits your website shop.

Examples of successful as well as unsuccessful authentications are shown.

The examples use customised pages rather than the defaults.

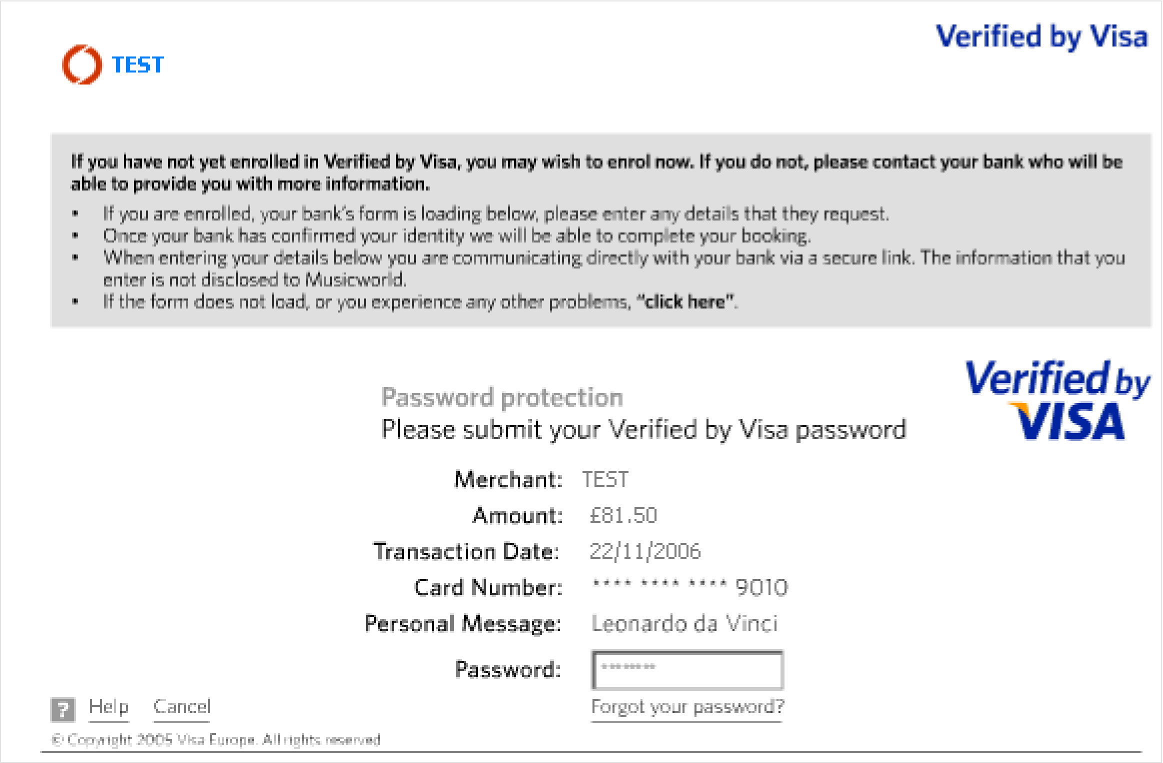
The overview reflects the process from the viewpoint of a standard merchant account, where our Risk Management service is used. In the case where a merchant supplies their own authentication service and their own risk management solution, the process may differ, especially if authentication fails.

3.3.1 Successful authentication

Although a Visa cardholder is used in this example, cardholders making a payment with MasterCard, Maestro, or American Express follow an almost identical process.

1. After deciding to buy, the cardholder selects the Buy button and the Payment Selection Page is displayed. The cardholder selects Visa as a method of payment. The Payment Page appears.
2. The cardholder completes their details and selects the Submit button.
3. The authentication dialogue page from the issuer is displayed. The cardholder checks their details and enters a personal password agreed with their card issuer before selecting the Submit button.

Help is provided by the card issuer if the cardholder cannot remember their password. Wording and layout on the authentication page is managed solely by the card issuer.



If you have not yet enrolled in Verified by Visa, you may wish to enrol now. If you do not, please contact your bank who will be able to provide you with more information.

- If you are enrolled, your bank's form is loading below, please enter any details that they request.
- Once your bank has confirmed your identity we will be able to complete your booking.
- When entering your details below you are communicating directly with your bank via a secure link. The information that you enter is not disclosed to Musicworld.
- If the form does not load, or you experience any other problems, **"click here"**.

Password protection

Please submit your Verified by Visa password

Merchant: TEST

Amount: £81.50

Transaction Date: 22/11/2006

Card Number: **** **** **** 9010

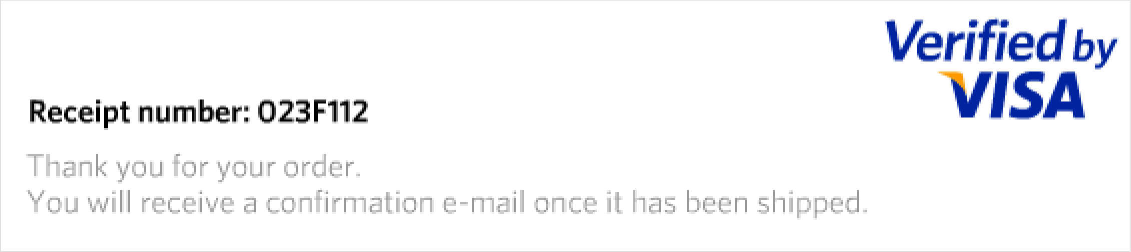
Personal Message: Leonardo da Vinci

Password: ********

© Copyright 2005 Visa Europe. All rights reserved

4. If the cardholder is successfully authenticated by their card issuer, we send the payment for authorisation. Following successful authorisation, the Results Page is displayed, as shown below. This process takes only a few seconds.

You can configure the Results Page, so the versions you see may be very different to this example.



Receipt number: 023F112

Thank you for your order.
You will receive a confirmation e-mail once it has been shipped.

5. The results of authentication appear in:

- The Payment Notification
- The Confirmation email
- The Merchant Interface Payment Page and Payment and Order Details Page
- The Merchant Interface Get Statement report

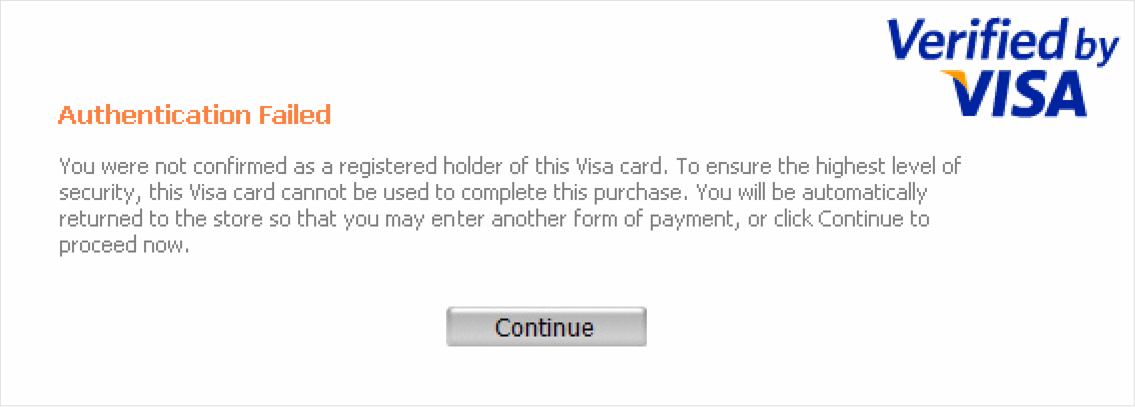
For further details about the authentication results, see **Managing and Interpreting your Authentication Results**.

3.3.2 Unsuccessful authentication

If a cardholder submits a wrong password, then they will fail to be authenticated by their card issuer. The card issuers will serve a message similar to the one shown below.

When a cardholder fails to be authenticated, the payment does not continue to authorisation. However, a record of the transaction exists and is available for examination in the Merchant Interface.

Also note that this process may differ where a merchant supplies their own authentication service and their own risk management solution.



Authentication Failed

You were not confirmed as a registered holder of this Visa card. To ensure the highest level of security, this Visa card cannot be used to complete this purchase. You will be automatically returned to the store so that you may enter another form of payment, or click Continue to proceed now.

4 Managing and interpreting your authentication results

4.1 Authentication results

Authentication results are displayed for the following:

- Payment Response
- Confirmation email
- Merchant Interface, in the Customer Interaction field on the Payment Details page
- 3D Secure result in the Get Statement

One of the following authentication results will be displayed for a MasterCard, Maestro, Visa, or American Express transaction. Note that in the Payment response, authentication results are indicated by a result number only. For example, the result "Cardholder Authenticated" is displayed in a notification as a "0" (zero), as follows:

```
authentication=ARespH.card.authentication.0
```

See **What is Liability Shift?** for benefits regarding the results.

Payment Response	Merchant Confirmation Email	MI Payment Details Page - Customer Interaction field	3DS Result configured in Get Statement Report	Explanation	Interpretation
0	Cardholder Authenticated	Cardholder Authenticated	Cardholder Authenticated	Cardholder entered their password correctly and their identity was successfully authenticated by the relevant card issuer.	High level of assurance as to the identity of the person making the transaction. This is a positive result.
1	Cardholder/ Issuing Bank not enroled for authentication	Authentication offered but not used.	Authentication offered but not used.	The relevant card issuer or cardholder is not enrolled.	This result provides no evidence about the identity of cardholder. Please refer to other fraud management results.
6	Cardholder Authentication not Available	Ecommerce	Authentication Unavailable.	Authentication was not possible due to a system or connectivity issue	This result is non-conclusive as a fraud indicator. Refer to other

Payment Response	Merchant Confirmation Email	MI Payment Details Page - Customer Interaction field	3DS Result configured in Get Statement Report	Explanation	Interpretation
					fraud-screening results.

You do not receive a result in the Merchant Interface when a cardholder fails to be authenticated by their card issuer. The payment does not proceed to authorisation.

4.2 How to interpret the results

The most significant result is "3D Used - Authenticated". It should give you confidence that the cardholder is truly who they say they are. However, although a result of "3D Used - Authenticated" is significant in verifying the cardholder's identity, it is important to your business that authentication results are combined with other fraud management results.

The other possible authentication results, such as, "3D Offered - Authentication offered but not used" or "Ecommerce", are less conclusive and you will need to rely on other fraud management results as well as your own fraud-prevention strategy.

5 What is liability shift?

Traditionally, merchants have been liable for e-commerce chargebacks due to fraud. Authentication brings the benefits of liability shift.

Liability shift means that the liability for the chargeback loss shifts from the merchant to the issuing bank, for e-commerce transactions that are deemed fraudulent (those transactions where the cardholder has denied involvement in the transaction). The issuing bank, in most cases, is no longer allowed to pass such chargebacks back to the merchant.

5.1 How has your liability for chargebacks changed?

From the date you are enabled for 3D Secure authentication you are no longer liable for certain fraudulent chargebacks when a cardholder denies they made the purchase. As a result, you should see a reduction in the number of fraud-related chargebacks.

Even if a transaction meets the criteria, the issuing banks can still chargeback for other reasons, such as non-delivery of goods or faulty goods.

5.2 Liability shift for personal cards and commercial cards

This table shows the eligibility of transactions for liability shift, involving both personal cards and commercial cards. These rules apply to Visa and MasterCard for any region, to American Express for SafeKey supported regions, and to JCB for J/Secure supported regions:

Scenario			Is the transaction eligible for liability shift?	Result
3D Secure	**Issuer participating**	Fully authenticated	Yes	Cardholder authenticated
		Attempted authentication	Yes	Authentication offered but not used
		Authentication failed	No	Authentication Failed
		Authentication error	No	Ecommerce
	Issuer not participating		Yes	Authentication offered but not used
Not 3D Secure			No	Ecommerce

5.3 Chargebacks and liability shift

For Visa, Maestro, MasterCard and American Express, card protection may be contingent upon the merchant taking reasonable measures to control fraud. If your fraud levels are unreasonably high you may forfeit the benefits of chargeback protection.

For more information about dealing with chargebacks, please refer to the **Disputed Payments Guide**.

6 Restrictions to authentication services

Some services and installations cannot use Authentication, such as those described below. The restrictions apply to MasterCard, Maestro, Visa and American Express cards.

Installation/service type	Reason
MOTO (WorldAccess)	This service does not qualify for authentication because cardholder details are not submitted to us by the cardholder. As a consequence, the cardholder cannot be queried for their authentication details. Thus, this service is not enabled for authentication. Accordingly, transactions deriving from this service, using these methods, are **not** passed for authentication.
Recurring Payments (FuturePay)	Authentication is only attempted on the first Recurring Payments transaction where the cardholder is present to enter their authentication details. All subsequent transactions are generated by you, the merchant, or by us, and as such, authentication is not attempted. If a cardholder changes their card details within the life of a Recurring Payments agreement and makes an immediate payment, authentication can be attempted. If there is no immediate payment, authentication is not attempted, as the cardholder is not present to enter their authentication details.
Checkout, Invisible and USA merchants	Although we cannot enable you for authentication we can advise on an individual basis when you contact us.
Merchants with an acquirer other than us	We can only enable you if we are your acquirer. If you are using a different acquirer you may need to contact them to become enabled, but please contact us in the first place.

Contact us

To find out more, get in touch with your Relationship Manager or:

- Email **corporatesupport@worldpay.com**