

ST Payment Pages

3-D Secure

Copyright

© SecureTrading 2008. All rights reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system or transmitted in any form or by any means whether electronic, mechanical or otherwise without the prior written permission of SecureTrading Ltd.

Disclaimer

This document is for informational purposes only. SecureTrading make no warranties, express or implied, through the distribution of this document. No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by SecureTrading, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

SecureTrading reserves the right to revise the content without obligation to notify any person of such changes.

Document revised on 13-Nov-2008. Document revision number 21.

Contents

1	Introduction.....	4
1.1	Overview	4
1.2	Brand schemes.....	4
1.3	Benefits.....	5
2	Using 3-D Secure	6
2.1	Switch/Maestro Changes	6
2.2	Signing up to the 3-D Secure schemes	6
2.3	ST Payment Pages and 3-D Secure	6
2.4	Viewscreens	6
3	Further information	8
3.1	Support.....	8
3.2	Further reading	8

1 Introduction

This document explains the 3-D Secure scheme and how to use this feature with SecureTrading Payment Pages.

1.1 Overview

3-D Secure is a protocol designed to reduce fraud and chargebacks during e-commerce Internet transactions. Cardholders are asked to identify themselves at the point of sale before the purchase can be completed. This usually means entering a PIN or other password after entering their credit card details.

In the event of a dispute with the transaction at a later date, the card issuer will usually take responsibility of the chargeback instead of the merchant.

SecureTrading offer this facility to merchants using Payment Pages for e-commerce transactions. For full details of the 3-D Secure protocol, see the [Further information](#) section.

1.2 Brand schemes

Various card brands have implemented the 3-D Secure protocol. Visa have a scheme called Verified by Visa and MasterCard have a scheme called SecureCode.

Each scheme works in a similar way, but each merchant must sign up with each scheme individually. Other card brands (such as American Express) are unaffected by the 3-D Secure protocol and as such these transactions do not gain any benefits.

1.3 Benefits

Benefits of the 3-D Secure process include the enhanced security available when performing a 3-D Secure transaction and the shift of liability in the event of fraudulent transactions. If a 3-D Secure transaction is completed and has been determined to be fraudulent then the credit liability is usually shifted from the merchant and onto the card issuer.

In most 3-D Secure cases the merchant will not receive any notification of a chargeback if the transaction is disputed by the cardholder. This is a major benefit in reducing lost revenue due to fraudulent transactions. Please note however, that 3-D Secure is not a 100% guarantee that no chargebacks will be incurred. There are some restrictions for each scheme although these cases should not occur very often.

SecureTrading believe the liability shift to be as follows:

Brand	Enrolled	Status	Liability
Visa	U		Merchant*
Visa	N		Card Issuer**
Visa	Y	Y	Card Issuer**
Visa	Y	N	Merchant***
Visa	Y	A	Card Issuer**
Visa	Y	U	Merchant
MasterCard	U		Card Issuer**
MasterCard	N		Card Issuer**
MasterCard	Y	Y	Card Issuer**
MasterCard	Y	N	Merchant***
MasterCard	Y	A	Card Issuer**
MasterCard	Y	U	Card Issuer**

*** Important note:** If the brand is Visa and the enrolled or status is returned as a “U” (Unknown) this means that the merchant is **not** covered by the 3-D Secure scheme. In this case the merchant is still liable for any fraudulent transactions.

**** Important note:** There are some cases where the liability is not covered by the Card Issuer; for example non-European commercial cards under both brands. For more information please contact your acquirer.

***** Important note:** In this case it is strongly recommended that the transaction does not proceed. This means the password entered did not match.

You should apply the same fraud detection/prevention measures to 3-D Secure transactions as you do to normal transactions.

The additional security benefits and liability shifts of 3-D Secure transactions are currently only supported by cards within the Visa and MasterCard brands. Any other issued cards (e.g. Solo, Amex) submitted as a Card Query request will respond with a result 2. They can only be authorised using standard authorisation methods.

To participate in the 3-D Secure scheme please contact support at support@securetrading.com.

2 Using 3-D Secure

To use 3-D secure with ST Payment Pages you must contact SecureTrading support. You will need your sitereference and acquirer information. This chapter assumes you are familiar with the basic setup of ST Payment Pages. Refer to the setup guide (see [Error! Reference source not found.](#)) for more information.

2.1 Switch/Maestro Changes

With Maestro debit cards replacing Switch cards, Switch cards will now be processed as Maestro debit cards on the SecureTrading payment system and you are required to submit “Maestro” in place of “Switch” for the card type when processing an authorisation.

A secondary change that MasterCard is enforcing is that all Maestro debit cards must use MasterCard SecureCode, current SecureTrading merchants will continue to be able to process Switch/Maestro cards as normal authorisations (Type: AUTH) but will be required to update their transaction processing so that all Maestro debit cards are processed using MasterCard SecureCode (Type: ST3DAUTH).

IMPORTANT: By processing Maestro debit cards after July 1st as normal authorisations, you may incur a fine from MasterCard.

Please contact SecureTrading support for more information.

2.2 Signing up to the 3-D Secure schemes

Some acquirers ask you to sign up with Verified by Visa and SecureCode by contacting them directly. Others prefer the sign up procedure to go via SecureTrading.

2.3 ST Payment Pages and 3-D Secure

Once you have signed up with one or more 3-D Secure schemes you may change your ST Payment Pages to use the new system. Once you have received confirmation of your enrolment in the scheme please contact SecureTrading support. You will need to provide your sitereference and your company name as seen by your customers on your website (maximum 25 alphanumeric characters). If you did not enrol in Verified by Visa via SecureTrading you will need to provide your VbV password. If your sitereference has multiple payment forms you can specify if only some of them should use the 3-D Secure scheme.

Please note that 3-D Secure is an e-commerce only protocol. It should not be used in situations where the cardholder is not entering their payment details directly (e.g. telephone sales).

No changes are required on your server to switch your account to use 3-D Secure. However, as with any change to a critical system you should monitor that transactions are processing as expected after the change has been made.

2.4 Viewscreens

After SecureTrading has confirmed your account is using 3-D Secure you will notice some differences in your transaction viewscreens. Some transactions (only those within the schemes for which you have enrolled) will show a transaction type of “ST3DAUTH” instead of “AUTH”. This shows the transaction was processed using the 3-D Secure protocol. Under normal conditions it should qualify for the liability shift. In addition extra fields are displayed when viewing individual transaction details. These fields include Enrolled, Status, Cavv, Eci and XID. These are values used by SecureTrading or provided by the issuer during the transaction. If you are contacted by the issuer regarding the

transaction you may be asked to provide this information. If you are asked for further details you may need to contact SecureTrading support.

If you do not see any ST3DAUTH transactions appear in your viewscreens after your account has been switched, please contact SecureTrading support.

It is possible that some transactions will appear as transaction type "AUTH" even though the card brand used would normally be covered by the 3-D Secure scheme. This can occur for several reasons, usually caused by a failure of one or more parts of the protocol. Your transaction may still be covered by the liability shift depending on the exact reason for the failure.

3 Further information

This section contains contact information relevant to SecureTrading Payment Pages

3.1 Support

SecureTrading provides support for its software and the operation of its payment service. If you require technical support, first ensure that you have read and understood all relevant documentation.

If the problem persists, please email support@securetrading.com, quoting your SecureTrading site reference and concisely stating the nature of your problem.

Note: Before sending any information to SecureTrading, care should be taken to remove any sensitive information, such as the credit card number.

SecureTrading additional contact details:

Phone: 01248 672 050

Fax: 01248 672 099

3.2 Further reading

For further information please refer to the following documents:

In the general setup guides (<http://www.securetrading.com/general-setup-guides.html>) section of the SecureTrading website:

- Going live document:

In the ST Payment Pages documents (<http://www.securetrading.com/payment-pages.html>) section of the SecureTrading website:

- SecureTrading Payment Pages setup guide

The full 3-D Secure specification is available from Visa

- <http://international.visa.com/fb/paytech/secure/main.jsp>

Verified by Visa

- <http://www.visaeu.com/iusevisa/shoppingonline.html>

MasterCard SecureCode

- <http://www.mastercardmerchant.com/securecode>
- <http://www.mastercardbrandcenter.com>