

How to protect yourself when trading online

November 2007

OFT959

The OFT has prepared the following advice for businesses who want to protect themselves, and their customers, when trading online.

As a business, you obviously want to make sure that you provide a safe and secure online shopping environment. This is in your best interests and those of your customers. Failure to do so can result in:

- increased business costs

your business can lose out from a fraudulent card transaction. Not only do you effectively 'sell' the goods without receiving payment, but you may also have to bear the administrative burdens of a chargeback when the genuine customer requests a refund from their bank or credit card company as a result of a fraudulent transaction on their account for goods they did not order

- reduced customer confidence and fewer transactions

OFT research suggests¹ that security fears can lead to consumers withdrawing from the market. They will be less likely to shop on websites when they have doubts about their security.

With these issues in mind, it is very important for your business to provide the most secure online trading environment possible, taking account of the cost of technologies, your potential fraud risk, and your likely turnover online, in order to protect both yourself and your customers. A secure e-commerce environment which promotes consumer confidence can be a real asset to your business.

¹ See the OFT market study of Internet Shopping (OFT921), available at www.offt.gov.uk for further details.

Security measures to help protect businesses trading online

All businesses selling online should use standard security measures such as SSL encryption when any personal information is entered by the customer.

If you are a very small business you may find that the best way to offer secure payments facilities is to use the services of a third party provider known as a Payment Services Provider or PSP. When the customer gets to the checkout stage they are redirected to a secure third party site to make their payment. Payment solutions of this type are provided by a number of well known firms that can be found using a search engine.

If your online business is large enough to want to process payments yourself you should seek the advice of your acquirer – the bank who provides your card accepting facilities – and they will be able to provide information on measures you can take to protect your business from fraud. For example, you should ensure that you use standard security measures such as the three digit Card Security Code and Address Verification Service. Furthermore, 'real time' payment systems can perform instant security checks and also take payment without revealing personal details to employees, lowering the risk of 'insider fraud'. There are also a variety of other commercial fraud tools available to suit different businesses. Details of these can be sought from your acquirer or found at www.cardwatch.org.uk where there is a wealth of training materials for retailers.

Secure online payment systems (known as Verified by Visa and MasterCard Securecode) are also available from your bank –these require the shopper to enter a passcode, to verify that they are the cardholder in a similar way to Chip and PIN, and can shift liability for fraudulent transactions away from the retailer and onto the issuing bank.

In addition to these technical solutions, 'common sense' manual fraud screening can be effective in picking up tell tale signs of fraudulent transactions. For instance, some retailers may choose to contact the purchaser and verify transactions where a large quantity of a good has been ordered to an address other than the billing address on the card.

You can find detailed information on how to protect your business from www.getsafeonline.org, www.businesslink.gov.uk and www.cardwatch.org.uk. Your own bank may also be able to offer advice.