# Barclaycard Payment Security case study

## Level 4 ecomm merchant data breach

In Sept 2013 a level 4 ecomm business in the baby products sector with pre-tax sales of circa £3m pa experienced a data breach via their web site, placing around 1,200 payment cards at risk.

In terms of the merchant's overall security status at the time of the breach, they considered their payment security status to be good, and that they were PCI DSS compliant. The merchant was using a fully hosted ecommerce payment solution and had previously attested to their compliance via SAQ-C, with ASV scans completed.

The merchant had a good level of awareness of the importance of data security and of the impact this can have on business: *"(Data security awareness) has always been very high and will always be. We know that sites can get a reputation for being porous."*

The merchant used a dedicated third party to host their website and database, and accepted online payments via credit/debit card and Paypal.

Barclaycard were alerted to the data compromise by Visa, and immediately made contact with the merchant. A forensic investigation subsequently determined that malicious web shells had been uploaded on the server by the compromise of a file up-load function within the blog section of the merchant's website.

The Barclaycard Payment Security team co-ordinated the remedial compliance activities required by the merchant, assisting them to re-validate their PCI DSS compliance, and to continue doing business in a secure environment as quickly as possible.

Around 1,200 unencrypted PAN details were found to be at risk, along with some additional stores of cardholder data which also needed to be erased as part of the remediation effort.

The impact of the breach on the merchant's business? *"We lost money on the sales refunded, lost the cost of buying test equipment, lost the cost getting the test done. It amounts to several thousand pounds."*

Merchants need to fully understand their card data environments and secure all the potential vulnerabilities of their payment acceptance processes, particularly in the ecommerce environment as any weakness are increasingly being targeted by fraudsters. If in doubt seek the services of a Qualified Security Assessor (see www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php)

## Barclaycard can help

If the worst should happen the Barclaycard Payment Security team are there to help, providing advice and assistance to ensure merchants undertake the necessary remedial activities to enable them to revalidate their PCI DSS compliance within the time frames stipulated by Card Schemes, avoiding the risk of further potential fines, and helping merchants to continue accepting payments in a secure and compliant environment.

For further help and advice please visit **www.barclaycard.co.uk/pcidss** or email **PCI.Taskforce@barclaycard.co.uk**

Barclaycard is a trading name of Barclays PLC. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register number: 122702). Registered in England. Registered No. 1026167. Registered office: 1 Churchill Place, London E14 5HP