

Card news – Keeping you in the know

Summer 2008 edition

It is important that you read, understand and act (where relevant) on the information contained in *Card news* as it may amount to variations in the terms of your card processing agreement with us.

New scheme mandate-security requirements for card not present merchants

From 1 December 2008, all merchants accepting card not present transactions whether by phone, mail order or internet must process ALL such transactions using the card security code (CSC) also known as CVC2 and CV2 and CVV2. Failure to do so could lead to scheme fines.

The card security code is the 3-4 digit code printed on the back of credit and debit cards – either on, or directly to the right of, the signature panel.

When the code is included in the transaction authorisation message, it can be checked by the card issuing bank. This indicates that the person making the transaction has access to the genuine card. By processing using this code you are reducing the risk of chargebacks and fraudulent transactions.

You must not store this code post authorisation, as this goes against the Payment Card Industry Data Security Standards (PCI DSS) rules on data storage.

All merchants using an HSBC Merchant Services' terminal already have this built into their solution. Anyone using alternative solutions should seek advice from their supplier about implementing this scheme requirement before 1 December 2008.

Card not present? Tips to reduce your chargeback risk

In a card not present (CNP) environment it is impossible for you to make a sale and be certain that it is the genuine cardholder using the card. But to help protect you against loss you may find the following tips useful:

- ▶ Always send goods by secure delivery to the requested address. Be cautious of transactions where the billing address is different to the requested delivery address. Do not release the goods to a third party e.g. a taxi or messenger. Tell couriers not to make the delivery if no one appears to live at the address.
- ▶ Where possible, perform card security code and address verification services checks. Refer to your terminal manual or supplier for assistance on using this security feature.
- ▶ If a customer requests to collect the goods, perform the transaction at the time of collection through your point of sale equipment.
- ▶ Be cautious of customers who give mobile phone numbers as their only form of contact.
- ▶ Be suspicious with transactions that have an unusually high value or volume for your type of business. Experience states these are likely to be fraudulent.
- ▶ Always refund transactions to the same card used for the original transaction.
- ▶ Keep a database of chargeback history to help identify patterns of fraudulent transactions. If a sale seems too good to be true then it might very well be.
- ▶ Do not be afraid to ask the cardholder further questions or request additional identification. Genuine customers will be pleased you are trying to protect them from fraud.

Essential points for preventing data compromises

Fraudsters attempt to obtain cardholder data by exploiting weaknesses when a transaction takes place or where the data is stored. By following the points below, the risk of compromise may be minimised:

- ▶ Treat paper copies of payment data e.g. transaction receipts, in the same manner as you would treat cash. Ensure that they are stored securely and only authorised personnel have access to such information.
- ▶ When data is no longer required, make sure paper copies are disposed of using a secure method such as cross cut shredding.
- ▶ With electronic payment data, ensure only personnel within the business that require transactional data have the ability to access that information. For example, staff may need to view cardholder names and addresses to fulfil orders, but the card numbers may be encrypted or truncated so that the full number is not visible if this is not required.
- ▶ The 3-4 digit card security code (CSC) also known as CVC2, CV2 and CVV2 must not be stored by merchants in either paper or electronic format.
- ▶ For system access, do not use passwords or user IDs that are generic or provided

by software suppliers as defaults. Do not access cardholder information, with shared IDs. They should be unique for each user. This also helps with audit trails.

- ▶ Where sensitive information is transmitted, the data should always be encrypted.
- ▶ Sensitive data should be protected from hacking attempts by a regularly maintained firewall.
- ▶ Anti-virus software should be used and kept regularly updated.
- ▶ System activity should be logged and readily accessible if required.
- ▶ Security systems and processes should be regularly tested.
- ▶ A policy should be maintained that addresses information security. All staff should be familiar with the relevant aspects of this policy.

Remember, if you are entrusting your payment information to a third party, then they also need to ensure that the above points are adhered to.

These points form the basis of the Payment Card Industry Data Security Standards (PCI DSS). Further information regarding PCI DSS can be found on their website: www.pcisecuritystandards.org