

# HSBC Merchant Services

***Card News*** – February 2009 Edition  
– keeping you in the know



Important information –  
Please keep this in a safe place

## New product available-Gift Card

For businesses with Sagem terminals and some integrated solutions



We have developed, and operate, a closed-loop Gift Card scheme. A closed-loop card scheme operates where the point of sale and redemption of the Gift Card are the same e.g. single retailer or chain, hotels etc.

- ▶ Available as an application on both an integrated solution or with your Sagem payment terminal
- ▶ Our Gift Card programme is tailored so as to be exclusive to your business
- ▶ Expert advice provided
- ▶ Business branded - cards styled by you to suit you
- ▶ Straight-forward packaged pricing
- ▶ Extensive management reporting and after sales support

For further details please contact our specialist partner, Card Commerce by telephone on 0870 735 2829 or by email at: [hmsgiftcard@card-commerce.com](mailto:hmsgiftcard@card-commerce.com).

## Pre-register now for new Electronic Management Information

Available for all Merchants



Introducing Electronic Management Information (eMI), a brand new business tool from HSBC Merchant Services enabling you to manage your business on every level.

eMI enables you to view online electronic reports of card processing transactions taken. Access is 24 hours x 365 days.

- ▶ Completely secure and easy to access
- ▶ Track up to 6 months worth of transactions
- ▶ Reports on all major card types including American Express and Diners Club
- ▶ Transaction data recorded from all (card) points of sale including e-transactions over the internet
- ▶ Filter and customise your own reports. You can export into Excel
- ▶ You gain greater control of costs and fraud.

eMI will be subject to a monthly fee included on your merchant invoice. The price will be tailored to your business needs.

eMI will be available to you with effect from June 2009. To pre-register your interest for eMI now, please call us on 0845 702 3344. Lines are open every day (except Christmas Day) 8am to 11pm Monday to Saturday. 10pm to 5pm on Sundays and 10am to 4pm on public holidays. Communications may be monitored and/or recorded.

### Revised pricing rates

We will be increasing some merchants' current card processing rates with effect from 1 April 2009. If you are impacted by this increase then you will have received a letter during February advising you of your revised card processing rates.

### Compliance Section

Keeping you safe



### Maestro SecureCode – You Need To Flow This Data Now

Impacted: All online merchants

We have referred to this mandate in previous editions of *Card News* and supported this with individual communications to many of you affected by it.

If you trade on the internet, accept Maestro debit cards and cannot flow Maestro SecureCode data, **You need to take immediate action now.**

**You must be able to flow this data by the end of February 2009.**

If you cannot do this for Maestro internet transactions, your transactions may be declined and you are likely to be fined **substantial** sums by MasterCard. The initial fine is expected to be US\$225,000 and then US\$25,000 per month thereafter whilst you are unable to flow this data.

Declined transactions will result in lost sales for your business.

If you decide **not** to flow this data, then you **must stop** accepting Maestro debit cards over the internet and remove all logos and Maestro references from your website. The mere presence of the logo if SecureCode data cannot be flowed may result in a significant fine.

Our recommendation is that you support 3D Secure (SecureCode and Verified by Visa - VbV) for all internet transactions and that you incorporate this into any development you do to support Maestro SecureCode.

A key benefit to you in supporting SecureCode is reduced exposure to chargebacks because fraudulent transactions become the responsibility of the Card Issuer.

We anticipate little or no flexibility by Maestro with this mandate or the fines and strongly urge you to take immediate action if you are impacted. Your first action should be to contact your service provider for guidance as soon as possible.

For clarification, this mandate is on the **merchant** to be able to flow this data; there is no mandate on Card Issuers or cardholders to actually use it (although this may follow). Regardless of whether the cardholder uses it or not when transacting with you, you receive the benefits from merely being able to support SecureCode. However increasingly, cardholders who are more aware of the risks when trading on-line, are actively looking for merchants to support 3D Secure transactions. Furthermore Card Issuers continue to tighten up their authorisation policies for non 3D Secure internet transactions as

they expect to see this being used.

## PCI DSS – Are you compliant? If not, why not?

Impacted: All merchants

We have referred to the requirements of the Payment Card Industry Data Security Standards (PCI DSS) in previous editions of *Card News* and many of you will also have received individual letters from us in respect of this initiative.

As a merchant, you are now obliged to ensure that any card data you process is safe and secure. In the event that card data is stolen, or hacked, from your systems and subsequently fraudulently used, you are liable for the subsequent losses and potentially unlimited fines from the card schemes. PCI DSS compliance will minimise the risks of card data compromise to your business.

More detail on the PCI DSS requirements can be found on the key website at:

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

Merchants categorised by PCI DSS as levels 1, 2 and 3 are now mandated to comply with the requirements. You will know if you are a level 1, 2 or 3 merchant as we will already have contacted you.

Later this year, a new mandate from one of the card schemes means that **any** merchant who trades over the internet and accepts e-commerce transactions, **must** be PCI DSS compliant. That includes **you** if you accept card payments over the internet.

We have already written to many of you in this regard and continue to work with SecurityMetrics, a Qualified Security Assessor (QSA), to move you towards compliance. Increasingly you can expect to receive more correspondence from us and them if you do not move towards a compliant status. We, as your card processor, will have to report your level of compliance to the card schemes. In the event that a non-compliant merchant suffers a data breach, there will be additional fines and costs. We will pass these fines on to you.

If you accept e-commerce payments and have not yet commenced a programme to become PCI DSS compliant, you need to take action now. You can start this process by contacting any QSA listed on the PCI DSS website or calling SecurityMetrics on 0844 561 1662 who will be pleased to assist you.

If you enrol with SecurityMetrics

there will be a small, preferential, charge for their service which has been negotiated with them by us. You will enter into a contract with SecurityMetrics which we are not party to and you will have to satisfy yourself regarding the terms of the contract. HSBC Merchant Services does not recommend the services of any individual third party supplier.

### Flowing Card Verification Value 2 (CVV2) data for Cardholder Not Present (CNP) Transactions

Impacted: All CNP merchants

Following on from previous articles in *Card News*, merchants who trade in a CNP environment are reminded of the need to flow CVV2 data with every telephone order and non 3-D Secure internet transaction. CVV2 is the three digit security code found on the reverse of a card, typically on or alongside the signature strip.

This **must** happen on every occasion where the cardholder is connected to or in contact with you at the time of the transaction and can therefore relay the CVV2 information for that specific transaction **and** the authorisation is carried out at the same time (to alleviate the need to store CVV2 as this is in direct breach of the PCI DSS requirements).

Failure to flow this data could result in transactions being declined by the Card Issuer or an increase in the number of chargebacks being experienced by you. Furthermore, failure to comply will result in escalating fines being levied on HSBC Merchant Services by the card schemes which **we** will pass on to **you**.

Please remember, however, that to maintain PCI DSS compliance (see article above) that the CVV2 data must not be stored by you in any format post authorisation.

The use of CVV2 data should give you increased confidence that your customer is genuine as this data can only be found on the physical card – i.e. your customer has to have the card to be able to access this data. However, we should remind you of the need to remain vigilant with these transactions and undertake your normal checks, as CVV2 does not offer any guarantee of payment or removal of liability

### Point Of Sale Security ~ Best Practice

Impacted: All face to face merchants

In the Winter 2008 edition of *Card News*, we highlighted the continued threat of fraudsters

seeking to compromise terminals/Personal Identification Number (PIN) pads in order to insert additional circuitry and obtain card data.

Additionally, we have now been alerted to a number of instances where the card presenter has temporarily retained control of the terminal to perpetrate a forced authorisation when an Issuer referral response has been generated.

Such incidences often involve the use of distraction techniques acted out by accomplices to divert the attention of the till operator.

In each case, following initial chip and PIN verification of the transaction amount, the card presenter conceals and then voids the 'Call Auth Centre' terminal display message, in the knowledge that their account is in excess of its available limit.

They then input a 'dummy' authorisation code, similar to that which otherwise would have been communicated by our Authorisation Centre Furnished with a printed terminal receipt embossed with the narrative chip and PIN verified and believing that the transaction has been approved the goods are handed over and the fraudsters depart the store.

Only when it is flagged up that the transaction has not been authorised does the deception come to light and the full magnitude of merchant liability to financial loss becomes apparent.

As the merchant, responsibility for the control and operation of the Card Processing terminal resides with you. Therefore due consideration should always be paid to the length of time you give to the cardholder to input their PIN details. Consideration should also be given to the security and positioning of your terminals. HSBC Merchant Services is investigating ways to help you combat this problem. Options being considered include terminal software upgrades, with password prompts where an Issuer referral is generated.

### **If you need to complain**

**Impacted: All merchants**

If for any reason you are not entirely satisfied with any aspect of our service, we want to hear from you as soon as possible. We will then make the relevant enquiries and aim to put matters right as soon as we can. Wherever possible, we will take steps to prevent the problem happening again.

Please begin by calling our HSBC Merchant Services card processing helpdesk on 0845 702 3344 and telling us where the problem has arisen. We will try to answer your concerns within 24 hours.

If this is not possible, we will endeavour to resolve your complaint within five working days. If we are unable to do this, we will write to you telling you how long our investigation is likely to take.

If you subsequently feel we have not resolved the problem to your satisfaction, you can write to our head office and your letter will be acknowledged within two working days of us receiving your letter.

Address your letter to:

The Customer Relations Manager  
Customer Relations  
HSBC Merchant Services LLP  
51 De Montfort Street  
Leicester  
LE1 7BB

Alternatively you can contact our Customer Relations team on 0116 281 8670, available 9.00am to 5.00pm Monday to Friday (except public holidays).

Our aim is to resolve all concerns internally. However if you are not satisfied with our response or if

eight weeks have passed since you first raised the matter with us, you may be able to complain to the Financial Ombudsman Service.

For further information about our process for resolving complaints please ask for our 'Complaints Information' leaflet.

### **The Financial Ombudsman**

The Financial Ombudsman Scheme deals with some types of complaints from small businesses (businesses whose annual turnover in the last financial year before the complaint is made is under £1 million).

Call: 0845 080 1800  
Email: [enquiries@financial-ombudsman.org.uk](mailto:enquiries@financial-ombudsman.org.uk)

Write to:  
The Financial Ombudsman Service  
South Quay Plaza  
183 Marsh Wall  
London  
E14 9SR

Or visit their website at  
[www.financial-ombudsman.org.uk](http://www.financial-ombudsman.org.uk)

