HSBC Merchant Services

MAY 2011 EDITION

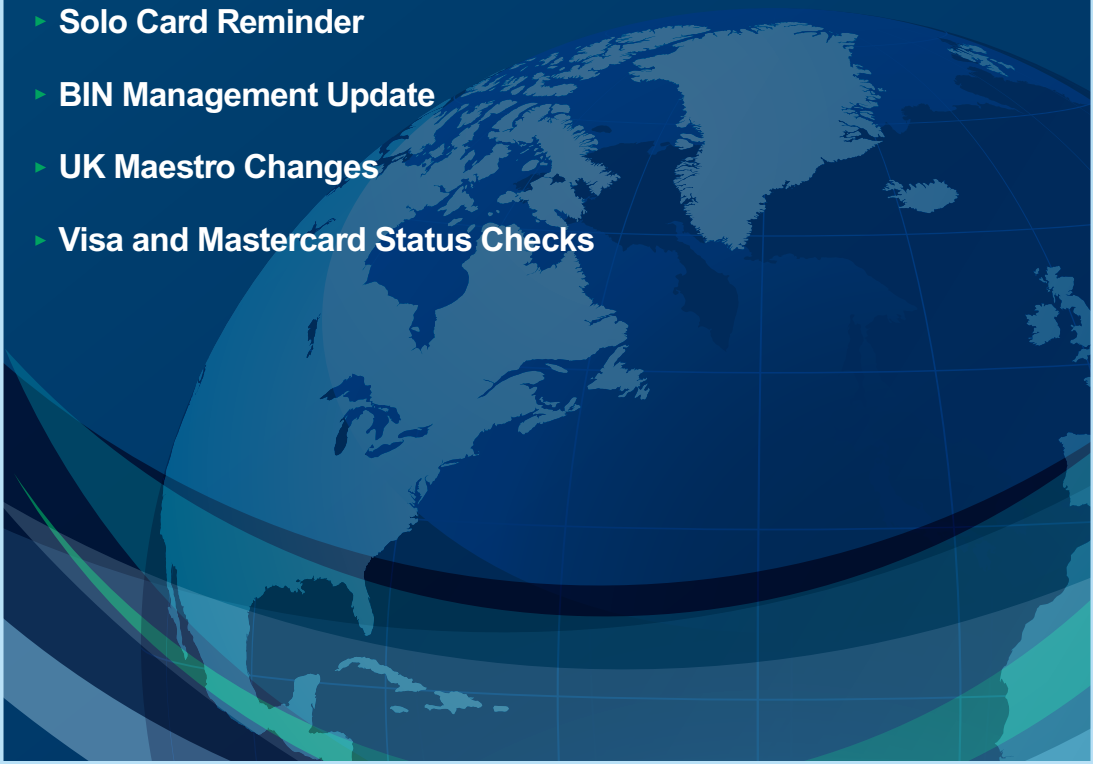
RETAIL SPECIFIC NEWS

Keeping you in the know

Important Information - Please keep in a safe place

This Edition of Retail Specific

- PCI DSS
- Solo Card Reminder
- BIN Management Update
- UK Maestro Changes
- Visa and Mastercard Status Checks



Tel: 0845 702 3344

globalpayments | HSBC

Compliance

Pharmacists and Tobacconists – BRAM – What You Need To Know

If you are a Pharmacist or Tobacconist and you offer prescription drugs or tobacco products for sale via the internet, mail order or by telephone (also known as non face to face or Card Not Present – CNP) you need to be aware of MasterCard's Business Risk Assessment & Mitigation (BRAM) mandate and how it impacts you.

If you offer prescription drugs or tobacco products solely in the card present environment, you are not affected by this mandate.

BRAM is intended to control and deter the use of MasterCard products (Maestro, Debit MasterCard and MasterCard Credit) in either illegal transactions or those that pose significant fraud, regulatory or legal risks.

If you wish to offer prescription drugs or tobacco products in the non-face-to-face environment and accept any MasterCard products, HSBC Merchant Services must register your business with MasterCard.

Registration costs approximately GBP 650* per year, which will be payable in advance, via a direct invoice. Merchants registering for the BRAM programme must also comply with the Payment Card Industry Data Security Standard (PCI DSS)** and maintain compliance with that programme when re-registering for BRAM.

Failure to register can incur significant fines from MasterCard. They can also demand that we remove your ability to accept their cards. It is, therefore, vitally important you comply with this mandate.

"Should you require further information on the BRAM programme please contact us on 0845 702 3344"

HSBC Merchant Services is in the process of contacting the Pharmacists and Tobacconists we provide card processing facilities to, in order to establish whether they need to register and to assist them with the relevant steps if required. If we haven't yet contacted you to discuss this, we will do so shortly.

Should you require further information on the BRAM programme please contact us on **0845 702 3344***** or visit www.mastercardacquirernews.com where an overview of the programme was published in the October 2009 edition of MasterCard's online publication The Acquirer. You can access this article by clicking on the link to the October 29 2009 edition found in the list of Previous Issues and selecting the BRAM Overview article from the list of highlights displayed.

"If you offer prescription drugs or tobacco products solely in the card present environment, you are not affected by this mandate"

*BRAM registration costs USD 1,000 per year. HSBC Merchant Services will convert this into GBP at the date of invoice, Card Scheme daily spot exchange rates for that day will apply for this conversion.

**For further information on PCI DSS please refer to the article contained in this edition of Retail Specific or visit the following website www.pcisecuritystandards.org.

***Lines are open between 9am and 6pm Monday to Friday excluding public holidays. Communications may be monitored and/or recorded. Any recordings remain our sole property. We also provide a Textphone service on **0845 602 4818**.

Expiration Dates For MasterCard Payment Systems And Visa Smart Debit/Credit Public Keys

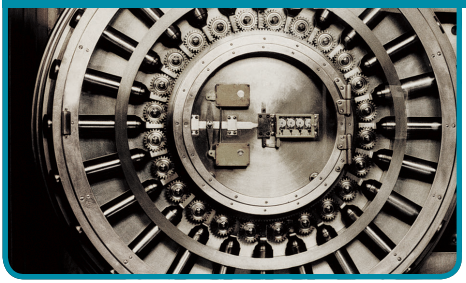
To maintain the highest level security of chip & PIN, there is a need to increase the level of encryption your Point of Sale equipment utilises.

If your terminal or Point of Sale equipment is provided by a third party supplier, you must contact them to confirm that all your terminals are loaded with an encryption key in excess of 1152 bit. Any terminals rented from HSBC Merchant Services have already been updated to take these changes into account and you do not need to update any of these you may have.

Failure to ensure your terminal uses the correct scheme public keys will result in the prevention of offline data authentication or offline enciphered PIN failures, and a reduction in your level of security.

Please see expiration dates for all active public keys:

- → 1024-bit expiration date 31st December 2009
- → 1152-bit expiration date 31st December 2017
- → 1408-bit expiration date 31st December 2020
- → 1984-bit expiration date 31st December 2020



Keeping card data secure - PCI DSS and compliance requirements

Under Card Scheme rules you are obliged to ensure you retain and process card data securely and employ a minimum security standard.

This minimum level of security is the Payment Card Industry Data Security Standard (PCI DSS). In previous editions of Retail Specific, as well by direct communications, we have made you aware that by failing to comply with this standard, you could not only be more exposed to the theft of card data, but also investigation by the Card Schemes and possibly significant fines.

Under the Card Scheme rules, some merchants (as detailed below) are mandated to be PCI DSS compliant:

Level One Merchant

- → Merchants who process more than 6 million card transactions per year for any Card Scheme (for example more than 6 million Visa card transactions per year or more than 6 million MasterCard transactions per year);
- → or a Merchant that has suffered a data compromise.

Level Two Merchant

- → Merchants who process between 1 million and 6 million card transactions per year for any Card Scheme (for example 2 million Visa card transactions per year).

Level Three Merchant

- → Merchants who process between 20,000 and 1 million e-commerce card transactions per year for any Card Scheme (for example 35,000 e-commerce MasterCard card transactions per year).

Level Four Merchant

- → Merchants who process less than 20,000 Visa or MasterCard e-commerce transactions per year or any other merchant not included within the definitions of Level One, Two or Three regardless of acceptance channel.

"As we advised in the last edition of Merchant News, the PCI DSS standard has been revised and reissued"

Changes To The PCI DSS Standard

The PCI DSS standard has recently been revised and reissued. The changes to the standard are minimal and, in most cases, are either a clarification of the existing requirements or the regulation has been expanded to provide additional guidance.

The new standard (2.0) came into force on 1 January 2011 but accreditations can be completed against the current version (1.2) until 31 December 2011.

Further information on the revisions to the standard is available from the PCI Security Standards Council website at www.pcisecuritystandards.org which we would encourage you to visit.

The website has been completely updated and now includes a specific section for merchants which we would encourage you to visit – this is easily accessible from the home page by clicking on the link.

"Under Card Scheme rules you are obliged to ensure you retain and process card data securely and employ a minimum security standard"

Level 4 E-commerce Merchants MUST Be Compliant

Level 4 e-commerce merchants – merchants accepting card payments via the internet – must be PCI DSS compliant.

This means that if you accept card payments via the internet you must comply with the PCI DSS standard and, by default, any third parties you use to process your payments must also be compliant.

Non-compliant merchants are at a significantly greater risk of a card data breach and the consequential associated costs that can ensue if a breach occurs.

These costs can and do, run into tens of thousands of pounds. We currently have a case on our books where a non-compliant Level 4 merchant has been breached and is likely to have costs over USD 128,000 (about £85,300) applied as a result of the breach.

In addition, if you are a non-compliant Level 4 e-commerce merchant, you are likely to be charged a non-compliance fee by us. The fee applies whether you are currently non-compliant or at any time you fail to renew your compliance, which must be done annually. You may have already noticed this on your monthly invoice and we will have written to you directly if you are impacted by this.

"Non-compliant merchants are at a significantly greater risk of a card data breach and the consequential associated costs that can ensue if a breach occurs"

Ensuring your business is compliant can generally be achieved for less than the non-compliance fee, which is currently £20 per month and which will increase in 2011 to cover the increasing costs we incur from non-compliant merchants.

Annual charges for compliance start from £11.99* per annum. If you accept card payments online but you haven't yet enrolled into the compliance program, you can enter into an arrangement with SecurityMetrics, the Qualified Security Assessor (QSA) we have been working with or, alternatively you can select another QSA of your choice. SecurityMetrics can be contacted on **0844 561 1662**† or via their website at www.securitymetrics.com.

Coming Soon – New Product For Card Not Present Transactions

The industry is seeing a slow migration of card fraud and data breaches into the Card Not Present (CNP) sector. Typically, CNP transactions (non face-to-face) are made by mail order, online or telephone.

If you accept cards in this way, we encourage you to familiarise yourself with the PCI DSS standard and ensure you operate at this best practice minimum level. Your failure to do so could, result in significant fines imposed by the Card Schemes should your card data be breached.

To ensure merchants accepting CNP transactions are properly protected we are developing a new product for launch later in the year to ensure your PCI DSS compliance.

We plan to provide customers who are impacted by this, with more details on this initiative later in 2011 by way of correspondence and updates.

Changes To The PA-DSS Standard

The Payment Application Data Security Standard (PA-DSS) has also been revised and reissued. The changes to the standard are minimal and are either a clarification of, or provide additional guidance on existing regulations.

As with PCI DSS the new standard (2.0) came into force on 1 January 2011 but accreditations can be completed against the current version (1.2) until 31 December 2011.

If you use, or intend to use, off-the-shelf software to capture and / or transmit payment card data you must ensure this is fully compliant with the PA-DSS requirements by 1 July 2012 in line with PCI-DSS compliance regulations.

Approved software is listed on the Card Scheme and PCI websites. Please contact your software vendor for guidance if you are unsure of the impact this may have on you, bearing in mind that if your vendor is not compliant, you could face fines.

Further information on the revisions to the standard is available from the website at www.pcisecuritystandards.org which we would encourage you to visit.

“Approved software is listed on the Card Scheme and PCI websites”

Use Of Third Party Agents

For most small and medium sized businesses the most cost effective route to trading online is to engage the services of one or more third party service providers. This can range from the organisation hosting the website to the payment service provider capturing and submitting the card payment data. This can leave card payment data vulnerable to a security breach.

If you are considering using a third party service provider for trading online there are several precautions you need to take when selecting and integrating the services of your chosen service provider(s) that can reduce the risk of the card payment data being compromised.

Most third party service providers will be within the scope of either the Payment Card Industry Data Security Standard (PCI DSS) or Payment Application – Data Security Standard (PA-DSS) (See above for more on these standards.)

To ensure your compliance with the PCI DSS standard, any third parties you employ to process transactions must be compliant and, where appropriate, PA-DSS compliant. This includes anyone that sees, processes or stores card data on your behalf.

In addition we strongly recommend that you;

- → Regularly check your website for any new or unknown web-pages or files. This should include checking that the code which redirects customers to your payments page is the same as the one originally supplied with your system and that it has not been modified.
- → Where a payments page is integrated into a shopping cart, ensure that it is patched to the most up-to-date version available.
- → Regularly seek advice from third parties to ensure your systems are appropriately secured. This is also to check that web and database servers are hardened to disable default settings and any unnecessary services.

Passwords And SQL Injection

The two most frequent causes of data security breaches are the use of default passwords and Structured Query Language [SQL] Injection Attacks, but you can reduce this risk.

Manufacturers of 'Point of Sale' devices often supply equipment with default passwords. Often, these have been published on the internet and have been used by hackers to gain illegal access to systems. You can reduce the risk of this by changing manufacturers default usernames and passwords as well as by using complex passwords, changing passwords frequently and limiting the number of incorrect password attempts.

An SQL (the database systems programming language) Injection Attack is when a retailer's database is infiltrated remotely and customer data extracted. Steps that should be taken to mitigate the risk of such an attack include constraining user input, using stored procedures and parameterised queries, identifying and mitigating vulnerabilities.

In view of the increased risks associated with the use of third parties, the Card Schemes are increasingly focused on them and actually require their members to ensure that they register third party agents with themselves.

We may need to enlist your help with this process, especially if you have a bespoke contract with a third party, however we will contact you directly if we require your assistance with this.

You should also be aware that if any of these third parties suffer a data breach, the fines are potentially more severe than a direct merchant breach.

Should you require any further information on any of the above, please call us on **0845 702 3344****, or visit the following websites:

- → https://www.pcisecuritystandards.org
- → http://www.visaeurope.com
- → http://www.mastercard.com

†Lines are open Monday to Friday, 9am to 5pm

*Fees start at £11.99 for merchants who have fully outsourced to a third party processor and from £74.99 for the first IP address used by merchants trading on the internet (subsequent IP addresses will incur a reduced fee)

Lines are open between 8am and 6pm Monday to Friday excluding public holidays. Communications may be monitored and/or recorded. Recordings remain our sole property. We also provide a Textphone service on **0845 602 4818.

"The two most frequent causes of data security breaches are the use of default passwords and Structured Query Language (SQL) Injection Attacks"

Decommissioning Of Solo – Reminder

In recent editions of our Merchant News publication, we have informed you that both HSBC Bank plc and Royal Bank of Scotland Group (RBSG) have ceased issuing Solo cards and that the scheme closed on 31 March 2011.

Whilst both banks replaced their Solo cards before the end of December 2010, a number of RBSG Solo cards are not due to expire until later in 2011.

This means that a cardholder may still present their Solo card to you for the first few months of 2011.

The authorisation system for Solo cards was switched off on 28 February 2011 and any cards submitted for authorisation after this date will be automatically declined.

If you are presented with a Solo card, or, you inadvertently accept one and receive a decline message, you must ask your customer for an alternative means of payment.

On 31 March 2011 The Processing Facility For These Cards Closed And No Further Processing Can Take Place.

If your terminal is supplied by a third party supplier, or you use a Payment Service Provider to accept internet payments, please contact them to ensure that they are able to meet these requirements.

Terminals rented from HSBC Merchant Services have already been updated to take these changes into account and you do not need to do anything.

If you have any queries regarding this, please contact our Helpdesk on **0845 702 3344***.

*Lines are open between 8am and 6pm Monday to Friday excluding public holidays. Communications may be monitored and/or recorded. Recordings remain our sole property. We also provide a Textphone service on **0845 602 4818**.

Solo & UK Maestro BIN Management Update

As part of their withdrawal from the UK Maestro and Solo card schemes, the HSBC Bank plc and RBSG Maestro and Solo card Bank Identification Numbers (BINs) listed below must be removed from all card terminals by 31 March 2011.

BINs		
→ 493660 - Maestro	→ 675965 - Maestro	→ 676754 - Solo
→ 493668 - Maestro	→ 675966 - Maestro	→ 676755 - Solo
→ 493698 - Maestro	→ 675967 - Maestro	→ 676756 - Solo
→ 630485 - Maestro	→ 675968 - Maestro	→ 676757 - Solo
→ 630498 - Maestro	→ 675969 - Maestro	→ 676758 - Solo
→ 671884 - Maestro	→ 675970 - Maestro	→ 676759 - Solo
→ 671886 - Maestro	→ 675976 - Maestro	→ 676760 - Solo
→ 675901 - Maestro	→ 675998 - Maestro	→ 676761 - Solo
→ 675918 - Maestro	→ 676703 - Solo	→ 676762 - Solo
→ 675924 - Maestro	→ 676708 - Solo	→ 676798 - Solo
→ 675938 - Maestro	→ 676709 - Solo	→ 676819 - Maestro
→ 675939 - Maestro	→ 676710 - Solo	→ 677117 - Maestro
→ 675940 - Maestro	→ 676711 - Solo	→ 677118 - Maestro
→ 675950 - Maestro	→ 676718 - Solo	→ 677119 - Maestro
→ 675960 - Maestro	→ 676740 - Solo	→ 677120 - Maestro
→ 675962 - Maestro	→ 676750 - Solo	→ 677121 - Maestro
→ 675963 - Maestro	→ 676751 - Solo	→ 982612 - Maestro
→ 675964 - Maestro	→ 676752 - Solo	→ 560398 - Maestro
	→ 676753 - Solo	→ 633311 - Maestro

If your terminal is supplied to you by HSBC Merchant Services, or you use our Secure ePayments service, we will manage the removal of these BINs and no further action is required by you.

If your terminal is supplied by a third party supplier or you use a Payment Service Provider to accept internet payments, you must contact them directly to confirm what action you are required to take to remove the above BINs.

If you have any queries regarding this change, please contact our Helpdesk on **0845 702 3344***.

*Lines are open between 9am and 6pm Monday to Friday excluding public holidays. Communications may be monitored and/or recorded. Recordings remain our sole property. We also provide a Textphone service on **0845 602 4818**.

UK Maestro Changes - May 2011

MasterCard have mandated that from 13 May 2011 the acceptance and processing of UK Maestro debit cards will be aligned with their standard Global Maestro card.

This alignment will see some features of the UK Maestro card being retained, however others will be removed. Details of these changes are listed below:

Features Being Demised

→ Paper Fallback Vouchers

You will no longer be able to use the fallback option of using paper vouchers to process Maestro transactions. This means that if your terminal is not operational, or does not accept the card, you must ask the cardholder for an alternative form of payment for this card

→ Key Entry For Purchase with Cashback

As advised in the March 2011 edition of Merchant News, you will no longer be able to perform a Purchase with Cashback transaction by key entering the card number on your Point of Sale equipment / terminal. From 1 March 2011 these transactions will be declined. All transactions supporting Purchase with Cashback must be processed using a chip and PIN transaction.

→ Key Entry For Customer Present Transactions

You will no longer be able to key enter customer present transactions. This means that if your Point of Sale equipment / terminal does not accept the card, you must ask for another form of payment.

→ Card Not Present Transactions Card Details – Issue Number

Maestro cards will no longer contain an Issue Number, so you are no longer required to collect this information as part of a card not present transaction.

"Maestro cards will no longer contain an Issue Number, so you are no longer required to collect this information as part of a card not present transaction"

→ Hot Card Files

MasterCard have withdrawn the requirement to provide UK Maestro Hot Card Files and as such HSBC Merchant Services will no longer provide these to polled (offline) terminals or mailboxes. As with the current rules, all non-chip read Maestro transactions will be subject to an online authorisation which will allow the Card Issuer to check the validity of each card transaction.

→ Reward Payments

Reward Payments will no longer be paid to merchants for captured Maestro cards.

Features Being Changed Or Retained

→ Floor Limits For UK Issued Maestro Transactions

Floor limits for UK Maestro transactions will be aligned to MasterCard Credit Card limits and all non-chip transactions (Mail Order / Telephone Order and eCommerce transactions) will continue to operate at zero floor limits.

If your terminal or Point of Sale equipment is provided by a third party supplier, or you use a Payment Service Provider to accept internet payments, you must contact them directly to confirm what action you are required to take to ensure your floor limits are aligned.

→ Cardholder Not Present And Mail Order/Telephone Order Transactions For UK Issued Maestro Cards

You will still be able to accept UK issued Maestro Cards for mail order and telephone order transactions; however this facility remains unavailable for Maestro Cards issued outside the UK.

→ Foreign Currency – Card Present / Card Not Present

All card present Maestro transactions for the purchase of foreign currency must be completed using a PIN (subject to disability laws) or the transaction will be declined.

Purchases of foreign currency made over the internet must be supported by Maestro SecureCode.

→ UK Issued Maestro BIN Range 6759xx

Maestro cards issued in the UK will continue to be issued under the 6759xx BIN range.

→ Maestro SecureCode

Maestro (MasterCard) SecureCode remains a mandatory requirement for all Maestro ecommerce transactions and the existing rules will continue to apply.

→ Cardholder Activated Terminals (CAT)

Post-alignment Maestro cards can still be used at CAT terminals – unattended Point of Sale equipment, where the cardholder initiates the transaction. However if your CAT terminal does not have the capability to perform authorisations online, then you will no longer be able to accept Maestro cards in this way.

Maestro acceptance will still be allowed at those CAT terminals that can go for online authorisation, but these devices must support both offline PIN and Mag-stripe. Any CAT terminals which are not PIN capable will not be able to accept any Maestro cards.

If your CAT does not comply with this requirement, you must contact your terminal supplier directly to confirm what action you are required to take.

→ Refunds – A Reminder

Refund transactions for UK issued Maestro cards do not require an authorisation request. If a refund is sent on-line, i.e. an attempt is made to authorise it, the refund will be declined. All terminals or Point of Sale equipment provided by a third party should have already been upgraded to comply with this processing requirement. If you are unsure whether your Point Of Sale equipment is compliant or not, you should contact your supplier for further information.

What Does This Mean To Me And What Action Do I Need To Take?

If you manage your own terminal or Point of Sale equipment, please make certain you take the appropriate steps to ensure compliance with these changes.

If your terminal or Point of Sale equipment is provided by a third party supplier, or you use a Payment Service Provider to accept internet payments, you must contact them directly to confirm what action you are required to take.

HSBC Merchant Services will manage the configuration changes for any terminals, including our Secure ePayments service, that you may rent from ourselves and no further action is required by you with regards to these terminals.

In addition to the technical changes required, please give consideration to your procedures for accepting Maestro cards.

If you have any queries regarding this change, please contact our Helpdesk on **0845 702 3344***.

*Lines are open between 9am and 6pm Monday to Friday excluding public holidays. Communications may be monitored and/or recorded. Any recordings remain our sole property. We also provide a Textphone service on **0845 602 4818**.

Zero Amount Status Checks for Visa and MasterCard Transactions

Visa and MasterCard have announced details of their new zero amount Status Check service, the adoption of which is compulsory from mid-June 2011, for all merchants who currently perform low value (typically £1) authorisations to verify a cardholder's account.

From 14th June 2011, a Status Check – performed with a zero amount value - will enable merchants to verify a cardholder's account without reserving funds.

Please be aware that this new process does not apply to business sectors such as hotels and car hire where pre-authorisations are undertaken. The process for pre-authorising transactions will not change.

What Does This Mean To Me And What Action Do I Need To Take?

If your terminal or POS equipment is provided by a third party supplier, or you use a Payment Service Provider to accept internet payments, you must contact them directly to confirm what action you are required to take.

If you manage your own terminal or POS equipment, please make certain you take the appropriate steps to ensure compliance with these changes.

If you currently perform low value authorisations, to verify a cardholder's account, on a terminal rented from HSBC Merchant Services, we will contact you before 14th June to advise you of the steps you will need to take. You don't need to do anything at this time.

If you require further assistance please contact our helpdesk on **0845 702 3344***

*Lines are open between 9am and 6pm Monday to Friday excluding public holidays. Communications may be monitored and/or recorded. Any recordings remain our sole property. We also provide a Textphone service on **0845 602 4818**.

Did You Know?

Our Authorisation Service: 0845 770 0600

When calling for authorisation or in response to a referral or request to call, please use **0845 770 0600**. When you call, please have your merchant number and the card details available.

The line is open 24 hours, 7 day a week, 365 days a year. Calls to this number may be monitored and/or recorded.

Calls to other numbers may result in a failed call that you will be charged for.

HSBC Merchant Services LLP

Tel: 0845 702 3344
Textphone: 0845 602 4818

AC21411