globalpayments

SUMMER 2013 EDITION

# RETAIL SPECIFIC NEWS

Keeping you in the know

Important Information - Please keep in a safe place ►

## This Edition of Retail Specific

- **Dynamic Currency Conversion**
- **Card Scheme Updates**

Tel: 0845 702 3344

# Dynamic Currency Conversion

## Taking A DCC Transaction, What You Need To Do

With respect to MasterCard and Visa regulations, it is a compliance requirement that every cardholder whose card is eligible for Dynamic Currency Conversion (DCC), is given the option to pay in either the merchant's currency or their home currency (the currency in which the card is issued).

- → You must make cardholders aware that DCC is an optional service and that the cardholder has the choice to pay in their currency if they prefer to.
- → The cardholder's own billing currency (home currency) must be confirmed before authorisation takes place. The currency recognition software does this automatically.
- → Your pricing currency remains the default currency on any transaction. However, where an eligible card is identified, the cardholder will be given the choice to decide which currency to pay with – either their home currency or the local currency.
- → The DCC service is fully transparent—the merchant's pricing currency, the exchange rate, the rate margin, the rate source, the cardholder's home currency amount, and DCC provider are displayed on the receipt and, for eCommerce customers, on the web site payment confirmation page and in the payment confirmation email.
- → All relevant DCC information must be made available to the cardholder before the transaction is completed. This information is readily available to the cardholder on the receipt or, for eCommerce customers, on the web site payment page.
- → From time to time MasterCard and Visa audit merchants who are enabled with DCC to ensure these regulations are being followed.

**"Every cardholder whose card is eligible for DCC, is given the option to pay in either the merchant's currency or their home currency"**

globalpayments

## Questions You May Get Asked?

**Q:** What do you recommend?

**A:** We recommend you pay in your home currency. You will benefit from a transparent transaction using today's exchange rate.

**Q:** Where do the exchange rates come from?

**A:** The wholesale exchange rates are sourced from Reuters. They are updated early every day and are very competitive.

**Q:** What are the commission charges?

**A:** The commission charged is not an additional charge but it merely replaces the currency conversion charges normally applied by your bank or card issuer.

**Q:** What's best for me?

**A:** It's better for you to pay in your home currency because:

**1)** You get up to date rates of exchange and not a rate in one or two days time

**2)** Paying in your home currency gives you full transaction visibility, allowing you to make an informed decision about your purchase.

**3)** The rates applied to your transaction are very competitive.

**Q:** Is there a charge for this service?

**A:** No, the amount quoted is the amount that will be charged to your credit card. This amount already includes a highly competitive margin replacing what is normally applied by your bank or card issuer with the added benefit of today's wholesale rate of exchange by Reuters.

# Card Scheme Updates

## Public Keys – Do your terminals hold the full set?

All debit and credit cards containing a 'chip' rely on the Card Schemes (MasterCard and Visa) 'Public Keys' cryptography to validate the data necessary to authorise and verify transactions. It is vital that if you own your own Point of Sale (PoS) equipment or rent a terminal from a supplier other than Global Payments, your equipment contains the latest set of 'Public Keys' to maintain an effective fraud prevention and detection capability.

Maintaining the correct Public Keys can benefit you by helping to minimise the time it takes to respond to an authorisation request. However, failure to maintain the correct set of Public Keys (which we've listed below) can not only increase the risk of fraud, it could also result in a higher than usual transaction decline rate, leading to customer dissatisfaction and loss of business.

Failure to keep your Public Keys up to date may result in a fine being applied to your account, so please take this opportunity to ensure the following is maintained;

1024-bit Public Key – Must not be deployed in new devices and should be removed from existing devices immediately.

- → 1152-bit Public Key – Should be deployed – Expiry date 31st December 2017.
- → 1408-bit Public Key – Should be deployed – Expiry date 31st December 2021.
- → 1984-bit Public Key – Should be deployed – Expiry date 31st December 2021.

If you have any questions or require details of the latest Public Keys, please call us on **0845 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. To help us continually improve our service, and in the interests of security, we may monitor and/or record your telephone calls with us. Any recording remains our sole property. We also provide a Textphone service on 0845 602 4818.

## Payment Application – Data Security Standards (PA-DSS)

If you purchase off-the-shelf software for your Point-of-Sale (PoS) equipment you must ensure that your software is listed by both the Card Schemes (MasterCard and Visa) and the Payment Card Industry Security Standards Council (PCI SSC) as being PA-DSS compliant. Using software that is not PA-DSS compliant is in breach of PCI DSS compliance regulations and can make you susceptible to a data breach and potentially the loss of customer card data.

Non-compliant software should be upgraded immediately and then configured and maintained correctly.

To assist you with this, the PCI SSC has introduced the Qualified Integrators and Reseller (QIR) Programme, with the aim of providing integrators and resellers who install, sell or service payment applications with authoritative guidance and best practices on secure installation.

Any supplier that undergoes this training will be listed on the PCI SSC website giving you a 'go-to' list of global suppliers qualified to handle the secure installation, configuration and maintenance of your payment solution.

It's very much in the early days of the programme but going forward we should all benefit from improved security and help to achieve PCI DSS compliance.

If you are unsure if your solution is compliant please contact your software vendor or PoS supplier for further information. Additional information can also be found on the PCI PA-DSS website **www.pcisecuritystandards.org**

If you have any queries regarding PA-DSS please call us on **0845 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. To help us continually improve our service, and in the interests of security, we may monitor and/or record your telephone calls with us. Any recording remains our sole property. We also provide a Textphone service on 0845 602 4818.

**"The PCI SSC has introduced the Qualified Integrators and Reseller (QIR) Programme, with the aim of providing integrators and resellers who install, sell or service payment applications"**

## Potential Security Risk To Hybrid PIN Entry Devices

Visa have identified a potential security threat involving Hybrid PIN Entry Devices (PED).

Hybrid PEDs have a single card entry slot which reads both the chip and the magnetic stripe on a debit or credit card (sometimes referred to a park and swipe or deep dip readers).

Visa have identified a number of cases where fraudsters have modified Hybrid PEDs to add a skimming device into the card reader slot to take copies of the card's magnetic stripe.

Merchants using devices of this type must ensure that any replacement/swap stock held is stored securely to reduce the risk of fraudsters infiltrating their terminal stock and modifying PEDs or, replacing PEDs with modified units.

Merchants should also be vigilant over engineers attending their sites to replace Hybrid PEDs and should ensure that appropriate validation is performed on any identification that is shown.

Where possible, merchants should look to move away from the use of Hybrid PEDs at the earliest possible opportunity and replace any such devices with more secure PCI PTS (PIN Transaction Security) 2.0 or 3.0 accredited devices.

If you have any queries regarding this requirement you will need to contact your terminal supplier. If you have any queries regarding your card processing facility with Global Payments please call our helpdesk on **0845 702 3344*.**

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. To help us continually improve our service, and in the interests of security, we may monitor and/or record your telephone calls with us. Any recording remains our sole property. We also provide a Textphone service on 0845 602 4818.

**"Merchants using devices of this type must ensure that any replacement/swap stock held is stored securely"**

## Removal Of Pre PCI PTS Approved Devices

From 1st January 2013 the minimum approval level for PIN Entry Devices (PED) is PCI PTS (PIN Transaction Security) 1.0.

Any devices certified to the Visa PED standard must be removed from use immediately as they are no longer deemed to provide an adequate level of security to satisfactorily protect card holder data – including the cardholder PIN.

PCI PTS 1.0 devices can still be purchased and used up until 30th April 2014 after which only PCI PTS 2.0 or later devices may be purchased.

Customers continuing to use Visa PED certified devices will be more susceptible to their PEDs being compromised than those using the more secure PCI PTS approved devices.

If you have any queries regarding this requirement you will need to contact your terminal supplier. If you have any queries regarding your card processing facility with Global Payments please call our helpdesk on **0845 702 3344***.

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. To help us continually improve our service, and in the interests of security, we may monitor and/or record your telephone calls with us. Any recording remains our sole property. We also provide a Textphone service on 0845 602 4818.

**“Customers continuing to use Visa PED certified devices will be more susceptible to their PEDs being compromised than those using the more secure PCI PTS approved devices”**

## Thank You For Reading...

Global Payments would like to thank you for reading our latest version of Merchant News. We hope you enjoyed, if you have any questions about any of the content in this issue, then please call us on **0845 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. To help us continually improve our service, and in the interests of security, we may monitor and/or record your telephone calls with us. Any recording remains our sole property. We also provide a Textphone service on 0845 602 4818.

For more information about Global Payments please contact us on **0845 702 3344***, or visit our website: **www.globalpaymentsinc.co.uk.**

*Lines are open Monday to Friday, 9am - 6pm, excluding public holidays. To help us continually improve our service, and in the interests of security, we may monitor and/or record your telephone calls with us. Any recording remains our sole property. We also provide a Textphone service on 0845 602 4818.

**Global Payments is HSBC Bank plc's preferred supplier for card processing in the UK.**

Global Payments is a trading name of GPUK LLP. GPUK LLP is authorised by the Financial Conduct Authority under the Payment Services Regulations 2009 (504290) for the provision of payment services.

GPUK LLP is a limited liability partnership registered in England number OC337146. Registered Office: 51, De Montfort Street, Leicester, LE1 7BB. The members are Global Payments U.K. Limited and Global Payments U.K. 2 Limited. Service of any documents relating to the business will be effective if served at the Registered Office.