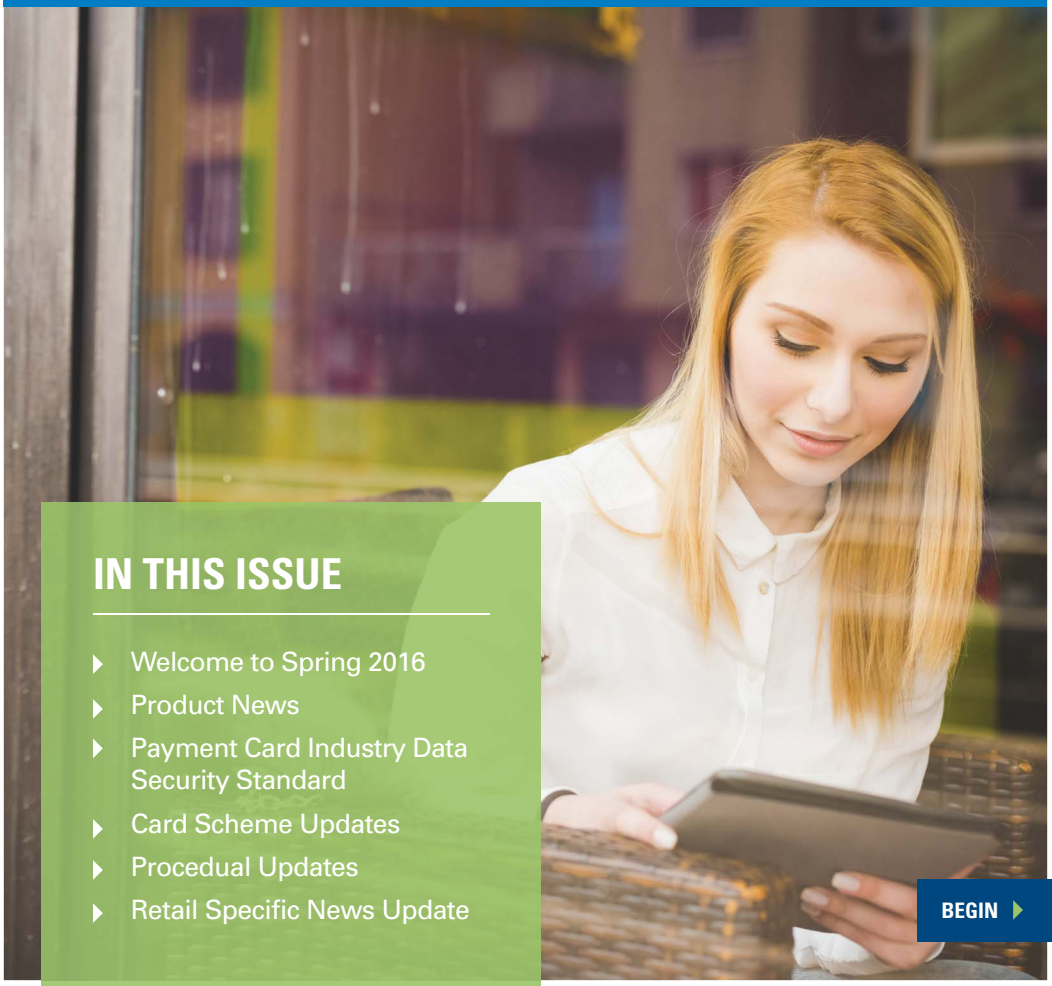
globalpayments

SPRING 2016

MERCHANT NEWS

INTERACTIVE EDITION - KEEPING YOU IN THE KNOW



IN THIS ISSUE

BEGIN

WELCOME TO THE SPRING 2016 EDITION OF MERCHANT NEWS

Chris Davies
President Europe

Nigel Hyslop
President and
Managing Director UK

In this first edition of Merchant News for 2016 I'm pleased to bring you updates from the Card Schemes and on the Payment Card Industry Data Security Standard. You'll also find articles on Product News and a section on Procedural Changes that you should read.

I'm really happy that our success with industry awards continues. At the Payments Awards held at the start of November 2015 we were winners in the 'Engagement And Loyalty Scheme Of The Year'. This award recognises our work with truRating, with us being the first card processor in the UK to integrate truRating's revolutionary customer rating service onto our terminals. You can find out more about truRating by visiting our website at: **https://www.globalpaymentsinc.com/en/unitedkingdom/accept-payments/management-information-tools/trurating**

Additionally, I'm pleased to share with you that in early February we joined the Home Secretary together with key representatives from the Government, law enforcement agencies and the banking sector, at the launch of the new Joint Fraud Taskforce. The taskforce will create a new era of collaboration, resulting in shared intelligence, a unified response and greater awareness of the risk of fraud among consumers.

I'd also like to take this opportunity to let you know about a major change that has taken place in Global Payments business in the UK. As my role within our business in Europe and Russia continues to grow, I've made the conscious decision to appoint someone to take over my responsibility for the UK business. It gives me great pleasure to announce that Nigel Hyslop has been promoted to President and Managing Director UK. He has almost 20 years' experience in the card payment industry, carrying out a number of different positions across the sector.

Going forward Nigel will be introducing the highlights in our Merchant News.

I'd like to close by wishing you continued success in your business endeavours.

All the best

Chris Davies
President Europe

NEXT

PRODUCT NEWS

HOMECURRENCYPAY IS CELEBRATING ITS FIRST BIRTHDAY

It's just over a year since we launched HomeCurrencyPay, our own Dynamic Currency Conversion (DCC) service, onto our Ingenico terminals and over the last 12 months we've processed over 1 million DCC transactions. Later this year we'll be adding HomeCurrencyPay to our VeriFone range of terminals, which'll allow even more of you to offer your international customers the choice to pay for their purchases in either sterling or their own currency.

If your terminal is set-up with HomeCurrencyPay it's worth remembering that:

- It helps broaden your business's appeal to international customers.
- There are no set-up or ongoing fees for this service.
- Online training is provided so you can become familiar with how it works.
- There's no change to the way you're credited.
- It can generate an additional revenue stream for your business with a monthly commission.

We're able to further complement HomeCurrencyPay with our Tax Free Shopping[1] service that allows your international customers from outside the EU to reclaim VAT made on non-consumable purchases over £30.

It's not too late to take advantage of both HomeCurrencyPay and Tax Free Shopping if you haven't already done so. Contact us on **0345 702 3344***, selecting the option for 'all other enquiries' and we can get you started.

[1]Tax Free Shopping is currently only available on our Ingenico terminals.

*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 0345 602 4818.

HomeCurrencyPay

CONGRATULATIONS TO KINGSTON UNIVERSITY

In the Summer 2015 edition of Merchant News we ran a competition giving you the opportunity to win an iPad by simply taking a HomeCurrencyPay transaction during August. From all the transactions that we processed that month, we're pleased to announce that our winning customer was Kingston University. The university donated their iPad to a prize draw for their students and here's a photo of Rob Pearce, the university's Finance Systems Manager, presenting the prize to the lucky winner Amanda Warth.

NEXT

GLOBAL PAYMENTS INTEGRATED SOLUTIONS JUST GOT A WHOLE LOT BIGGER!

DO YOU USE A TABLET TO SUPPORT YOUR BUSINESS?

Tablets are now common place and are used to support many businesses with bespoke applications including mobile Point of Sale functionality. The great news is that Global POS Link, our semi integrated solution, can now be developed over IP, which in simple terms means we can get our terminals talking to the apps running on your tablet. This will give you the normal benefit of integrated payments with no double keying, better customer experience and easier reconciliation with your tablet application!

It also means you can take advantage of the value added services we offer such as HomeCurrencyPay and Tax Free Shopping. This makes for an extremely flexible solution that can be used as your main point of sale, for a queue busting tool or a consultative sale as you can have another application open to showcase products, order stock, etc.

If you want to know more, why not visit our website at: **https://www.globalpaymentsinc.com/en/unitedkingdom/accept-payments/terminals/global-pos-link** or call us on **0345 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 0345 602 4818.

"The great news is that Global POS Link, our semi integrated solution, can now be developed over IP, which in simple terms means we can get our terminals talking to the apps running on your tablet."

HIGH VALUE PAYMENTS ARE COMING

Following the launch of Apple Pay, there's been a significant increase in the number of Near Field Communication (NFC) enabled mobile phones that are capable of making Contactless payments. As a result of this (and as Apple Pay will only be the first of many NFC payment methods) businesses that accept Contactless payments now need to enable High Value Payments (HVP) on their card terminals.

HVP are Contactless payments made on a mobile phone that are greater than the £30 limit for Contactless cards. However, they're protected by the cardholder verifying themselves via their phone, either by using a scanned thumb/fingerprint in the case of Apple Pay or by entering a pass code for other mobile phone manufacturers. This process is known as a Cardholder Device Cardholder Verification Method or CDCVM for short.

Once HVP is enabled, the Contactless logo will be displayed on your terminal for all transactions rather than just those under the £30 limit as happens currently. Acceptance of Contactless debit and credit cards for transactions up to the £30 limit will continue as normal. If a cardholder taps a Contactless card for a transaction above the £30 limit, the terminal will instruct them to complete the transaction using chip and PIN.

A HVP transaction performed via an NFC enabled mobile phone and verified using a CDCVM is as secure as a chip and PIN transaction and follows the same rules as a chip and PIN transaction for liability and chargebacks. In some cases, a cardholder may need to tap their mobile phone against the Contactless reader twice. This is because they've not pre-entered their CDCVM on their device prior to starting the transaction. Their device will prompt them to complete their CDCVM and tap the phone again to complete the transaction.

In order to accept HVP, terminals must be certified to Visa 2.1.1 Contactless specifications and MasterCard PayPass 3.0 Contactless specifications. If you rent a terminal from us you don't need to do anything as your terminal is already certified to the correct specifications and we'll be automatically upgrading it to activate HVP over the coming months. If you own your own terminals or rent them from a third party you'll need to contact your supplier to confirm that your terminals meet the required certification levels and ask them to turn on HVP.

If you have any queries regarding HVP, call us on **0345 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 0345 602 4818.

NEXT

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

ARE YOU PAYING PCI DSS NON-COMPLIANCE CHARGES?

PCI DSS is a globally adopted industry standard that sets out the procedures that must be adhered to, to ensure the safe storage, processing and transmission of payment card data. **All merchants are mandated to achieve and maintain PCI DSS compliance in accordance with Card Scheme Rules.**

If you remain non-compliant, in accordance with your Card Processing Agreement, we'll apply a monthly non-compliance charge of 15p per transaction or a minimum of £50 per merchant ID, for each month you remain non-compliant.

INTRODUCING GLOBAL FORTRESS

To help you achieve and maintain PCI DSS compliance we've developed Global Fortress in partnership with SecurityMetrics our Qualified Security Assessor (QSA). This gives you access to the resources you need to help you safeguard your customer data and avoid the monthly non-compliance charge.

You can find further details on PCI DSS in the Data Security section of our 'Know The Risks' brochure provided to you at set-up. If you need a new copy, please call us on **0345 702 3344*** selecting the option for 'stationery' and we will arrange for one to be sent out to you. Alternatively, you can download a version by logging into the 'Customer Centre' of our website **www.globalpaymentsinc.co.uk** and selecting the option for 'Global Payments', followed by 'Card Processing'.

You can also find out more about PCI DSS by visiting the Global Fortress website at **www.globalfortress.co.uk** or you can call SecurityMetrics directly on **0330 808 1003**** or **0203 014 7829****. If you'd prefer, you can request a call back from them by emailing **globalfortress@securitymetrics.com** and they'll talk you through the steps you need to take to achieve compliance.

Global Fortress

WHO ARE SECURITYMETRICS?

SecurityMetrics have more than 12 years' experience in helping businesses with their PCI DSS needs. They're one of only a few QSA's that offer all PCI services, which include:

- QSA services and PCI consultancy.
- Approved Scanning Vendor (ASV).
- Penetration testing.
- Onsite PCI Compliance audits (Report on Compliance - RoC).
- Security Metrics PANscan.
- Internal vulnerability scanning solution – SecurityMetrics Vision.
- Payment Application Qualified Security Assessor (PA QSA).
- PCI Forensic Investigator (PFI).

They have an award winning call centre that provides:

- An initial free consultation to confirm your PCI validation requirements.
- And once you're enrolled, provides unlimited technical support to assist you to understand and complete your requirements. So if you need help, just ask!

They also provide online glossaries and also publish videos on YouTube, all aimed at helping you to meet this ever evolving and important Card Scheme mandate.

WHAT HAPPENS ONCE I'M COMPLIANT?

Once you've achieved compliance, it's vital that you communicate any changes to your business to SecurityMetrics (or your chosen QSA, if you decide not to use SecurityMetrics). These include, but aren't limited to, the following:

- A change in the manner in which you process transactions or handle customer data, including changes with the third parties/ payment applications that you use.
- Obtaining new or additional merchant numbers.
- Any other updates such as a change of legal entity, contact details (name, address, email).

The Card Schemes monitor PCI DSS compliance closely and both SecurityMetrics and Global Payments may contact you by telephone, email or post to discuss your compliance.

*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 0345 602 4818.

**Lines are open Monday to Friday, 9am - 5pm. Calls may be monitored and/or recorded. Any recording remains SecurityMetrics sole property. Please consult your phone line provider for call costs to 0844 800 numbers. For guidance, BT residential rates are 5.105p per minute, plus a call set-up charge of 15p (current at February 2014).

"Once you've achieved compliance, it's vital that you communicate any changes to your business to SecurityMetrics (or your chosen QSA"

NEXT

PCI DSS – WHAT'S DIFFERENT IN VERSION 3.1 (V3.1)?

The PCI Security Standards Council released PCI DSS V3.1 on **1st July 2015**, which includes key changes that relate to the removal of Secure Sockets Layer (SSL), a method of strong cryptography. The updated version has been in effect since that date and is available from **https://www.pcisecuritystandards.org** It also includes revised Self-Assessment Questionnaires (SAQ's), an updated Report on Compliance (RoC) template and a modified Prioritised Approach Tool.

WHAT DO I NEED TO DO NEXT?

You'll need to validate your PCI DSS compliance against V3.1. If you've already validated your compliance then this will remain valid until your next renewal, although you should still look to upgrade your security as soon as possible. Your next compliance will be measured against PCI DSS v3.1, so you may wish to start planning for changes now.

Global Fortress is fully compliant with the PCI DSS V3.1 standards. If you've already signed up, our partners at SecurityMetrics will identify your requirements at your next renewal and will contact you if any changes need making.

If you're not using Global Fortress, you can find more information about the service in the previous article. Alternatively, call us on **0345 702 3344*** selecting the option for 'all other enquiries' or visit our website at **www.globalfortress.co.uk.**

WHAT ARE THE CHANGES IN PCI DSS V3.1?

There are 36 changes, most of which are clarifications and additional guidance. However, there are changes that directly reinforce the latest security protocols. These are:

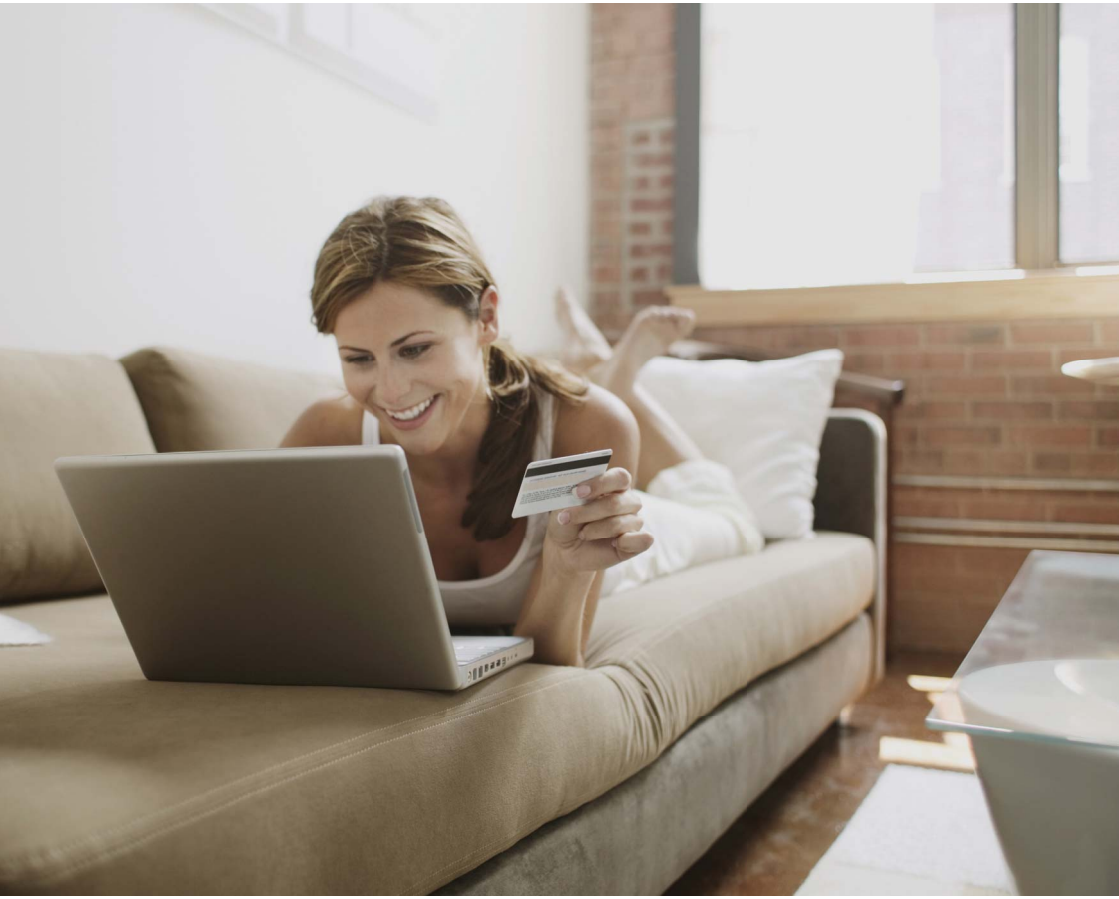
2.2.3 Implement additional security features for any required services or protocols that are considered to be insecure

2.3 Encrypt all non-console administrative access using strong cryptography

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

If you need further information regarding the PCI DSS standards you can visit **https://www.pcisecuritystandards.org/security_standards/documents.php.**

"There are 36 changes, most of which are clarifications and additional guidance. However, there are changes that directly reinforce the latest security protocols."



NEXT

PCI DSS – WHAT'S DIFFERENT IN VERSION 3.1 (V3.1)?

WHY IS SSL NO LONGER CONSIDERED SECURE?

If you connect to the internet over a network, you'll probably be using encryption protocols (SSL or Transport Layer Socket (TLS)). Their purpose is to secure the connection between two 'end-points', for example your customer's web-browser and the web-server that hosts your website, providing privacy and data integrity along the communications channel that flows between them.

Despite being in widespread use for several years, SSL 3.0 and TLS v1.0 are both now considered vulnerable to attack. One of the most high-profile weaknesses allows attackers to extract data from secure connections. Commonly referred to as POODLE (Padding Oracle On Downgraded Legacy Encryption), this vulnerability makes it possible to decrypt an encrypted message secured by SSL v3.0.

There are no known fixes for these flaws so SSL 3.0 and TLS 1.0 and TLS 1.1 are no longer considered as strong encryption methods. From **30th June 2018**, these protocols can no longer be used as a security control as web-browsers will soon begin to prohibit SSL connections to try and prevent connection to web servers that are vulnerable to attack. Whilst June 2018 is still some way off, if you're still using either SSL or TLS V1.0 or V1.1, you should look to disable these entirely and use a more modern method of encryption, with TLS V1.2 being the recommended standard.

PREV

WHAT TO DO IF YOUR DATA IS COMPROMISED

WHAT IS A DATA COMPROMISE?

A data compromise, or breach, occurs when an unauthorised person accesses your customer's information with the intent to commit fraud. The information of most value to criminals include your customer's card number, expiry date, name, address and the security details such as CVC code and the track data.

Criminals can gain access to your customer's cardholder information in many ways, including:

- Theft from premises of terminals and terminal receipts,
- Hacking of your website or computer network,
- A dishonest member of staff accessing and passing on cardholder information to criminals, or
- Through your Third Party Merchant Agents or service providers, such as your web hosting company, who may have not taken the necessary precautions to safeguard your customer's data that you have outsourced to them.

"The information of most value to criminals include your customer's card number, expiry date, name, address and the security details such as CVC code and the track data."

HOW DO I KNOW IF I'VE BEEN COMPROMISED?

Businesses become aware of a breach in many ways, such as through internal system generated incident reports, unusual or new web pages or files on their website, alerts through their Payment Service Providers and also from their cardholders reporting fraud. However, it's possible for a business not to realise that they've been breached at all as the criminals sometimes don't leave much evidence behind.

NEXT

WHAT SHOULD I DO IF I'VE BEEN COMPROMISED?

Data breaches cost the payment industry millions of pounds every year. For the compromised company, this can be a time of uncertainty and anxiety with the possibility of adverse publicity and large costs. If you suspect that your business has suffered a data breach, there are immediate steps you can take to minimise the possible damage and achieve compliance quickly.

- Call us on **0345 702 3344***, selecting the option for 'all other enquiries', immediately and report the incident.
- Notify the relevant law enforcement agency.
- To minimise further data loss, and preserve evidence and facilitate the investigation process, follow the below 'Do's' and 'Don'ts':
  - Don't access, alter or delete files in the compromised system(s).
  - Don't attempt to change passwords on the compromised systems.
  - Don't log in as ROOT.
  - Don't turn off the compromised system(s).
  - Do isolate the compromised system from the network, for example, unplug network cable.

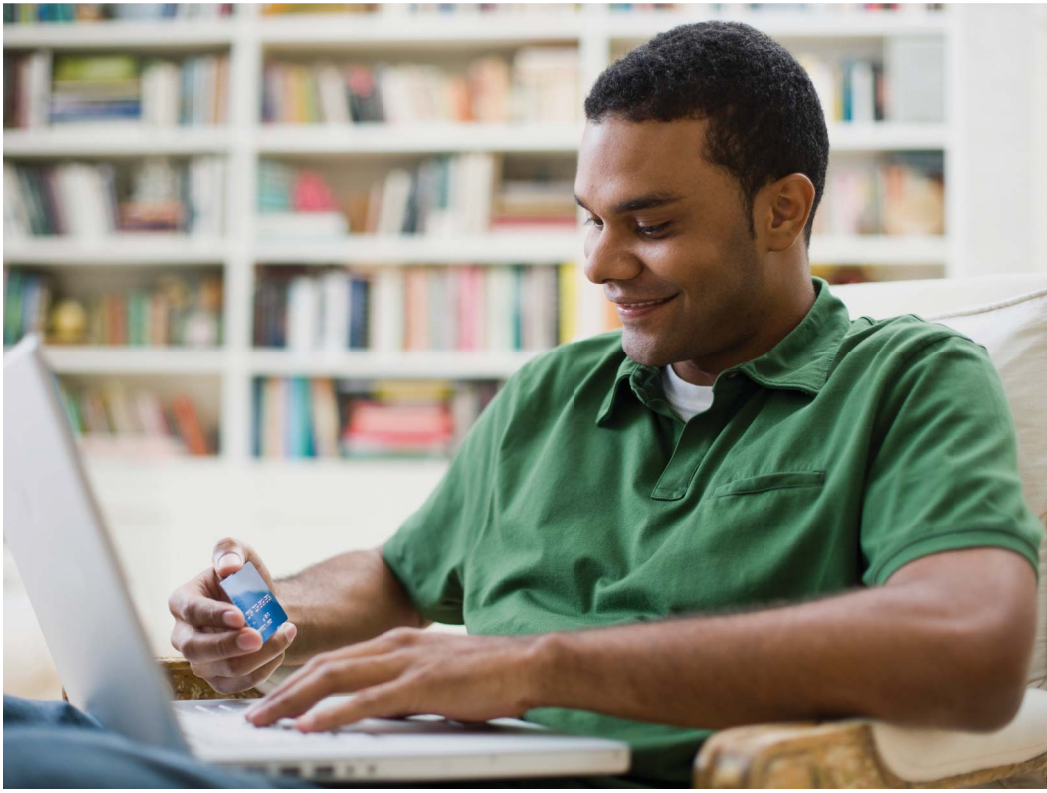
If access to the compromised system can't be avoided then keep detailed records of the action(s) taken with the dates and time.

- Do preserve logs, for example, security events, web, database, firewalls.
- Do change the Service Set Identifier (SSID) (if using a wireless network) on the wireless access point (WAP) and other systems that use WAP, with the exception of any systems believed to be compromised.
- Monitor traffic on all systems with cardholder data and be on 'high alert', ensuring you log all actions taken.

By self-reporting any suspected breach early you can help to reduce the impact to your business and may reduce the possible penalties from the Card Schemes. If in doubt, contact us immediately and report any incidents.

We can provide guidance and a dedicated contact to help you go through the next steps. We'll support you whilst you address the breach and achieve PCI DSS compliance so that your business is safe to continue to take card payments.

*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 0345 602 4818.



"By self-reporting any suspected breach early you can help to reduce the impact to your business and may reduce the possible penalties from the Card Schemes. If in doubt, contact us immediately and report any incidents."

NEXT

CARD SCHEME UPDATES

DON'T IGNORE STOP INSTRUCTIONS

In previous editions of Merchant News, we've made you aware that cardholders can instruct their card issuer to stop any of the following Cardholder Not Present (CNP) future dated payments:

- Recurring Transactions
- Instalment Transactions
- Payday Loan Repayments

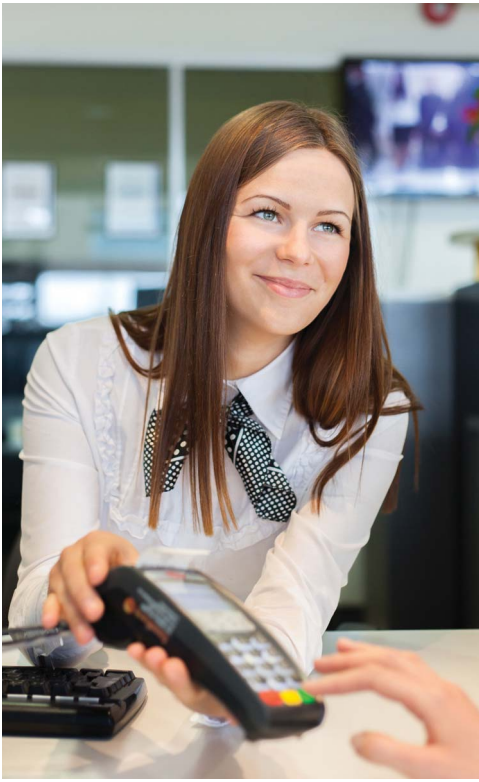
Attempting to authorise a card transaction that has a stop instruction against it will see the card issuer send back a decline response together with an accompanying description of 'Consent Revoked'.

Visa and MasterCard continue to monitor this service to identify any misuse. Please remember that if you receive a Consent Revoked decline response **under no circumstances should you attempt to re-authorise the transaction**. Instead you must contact the cardholder to discuss alternative payment arrangements.

If you have any queries regarding this, please contact us on **0345 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 0345 602 4818.

STATUS CHECKS



HOW DO YOU VERIFY YOUR CUSTOMER'S CARD?

Do you perform a low value authorisation, for example £1, to verify a cardholders account? If you do, did you know that Visa and MasterCard have banned this type of authorisation and that you're being charged a Processing Integrity Fee (PIF) for doing so?

You should be processing a Zero Value Status Check instead. These allow you to verify a cardholder's account without reserving funds from their available balance. It'll also ensure that you aren't being charged a Processing Integrity Fee. You can find out more about this fee in the MasterCard Authorisations article later in this section.

You can find more details on how to perform a Status Check in your terminal user guide or by calling us on **0345 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 0345 602 4818.

"You should be processing a Zero Value Status Check instead. These allow you to verify a cardholder's account without reserving funds from their available balance."

NEXT

"SAD is used during authorisation to check that the genuine cardholder has authorised the transaction and strictly can't be stored after the authorisation."

DO YOU KNOW ABOUT SENSITIVE AUTHENTICATION DATA (SAD)?

WHAT IS SAD?

Part of the process when accepting a card payment, whether the cardholder is present or not, is for you to seek authorisation from their card issuer. SAD is used during authorisation to check that the genuine cardholder has authorised the transaction and strictly can't be stored after the authorisation. SAD includes the following items:

- **Card Security Code (CSC)/Card Verification Value (CVV)**: This is a three or four digit validation code found on the back of a payment card, either within the signature strip or in a white box to the right-hand side of the signature strip. This is used to authenticate CNP transactions.
- **PIN Number**: This is used by the cardholder to authenticate a Card Present transaction, for example, at a card terminal in a shop.
- **Track Data**: This is contained within the magnetic stripe on the back of a payment card and is used when a card is swiped through a card terminal.

WHY CAN'T I STORE SAD AFTER AN AUTHORISATION?

As SAD is used by card issuers to verify and approve transactions, it's vital that this data is protected. Storing SAD after an authorisation has been attempted is against PCI DSS and Card Scheme Rules.

Storage of SAD post authorisation is not permitted under any circumstances including electronic storage and paper storage. Even if the data is encrypted or otherwise protected it should be securely erased or shredded.

There shouldn't be any need for you to store SAD after a transaction has been authorised. Storage of this data decreases the effectiveness of an authorisation and fraud detection systems in the authorisation process and can lead to increased credit card fraud if compromised. If you're compromised and SAD is stolen, the penalties for your data breach will be considerably increased.

GUIDANCE…

For further guidance on how to protect SAD and how to comply with PCI DSS, please take the time to visit the PCI Security Standards Council website at **www.pcisecuritystandards.org/index.php** or contact a Qualified Security Assessor (QSA). The website provides lots of information and supporting documentation regarding the requirements of SAD storage, together with general advice on how to achieve and maintain PCI DSS compliance. So we strongly recommend that you take the time to visit and review their website.

For general enquiries about PCI DSS, please call us on **0345 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 0345 602 4818.

NEXT

REMINDER: MANDATORY CHANGES – SCHEME REFERENCE DATA (SRD)

To aid the detection of card fraud and make the linking of chargebacks to their original transaction easier, Visa and MasterCard require a unique reference number to be flowed throughout the lifecycle of all authorised card transactions. Visa refers to this data as the Transaction Identification Number, whilst MasterCard refers to it as the Trace Identification Number. Generically this data is referred to as SRD.

If you use your own equipment or a Payment Service Provider (PSP) to accept card payments, you're responsible for ensuring that all transactions contain SRD. To assist you with this we have put together a Technical Specification document which details the changes you'll need to make. You can download a copy of the document and view a series of Questions and Answers by visiting our website at **http://www.globalpaymentsinc.co.uk/traceid.html** and clicking on the option for `Scheme Reference Data`. Failure to include the SRD could result in fines being levied by Visa and MasterCard, for which you will be liable.

If you have any questions about these mandatory changes, please call us on **0345 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 0345 602 4818.

"To assist you with this we have put together a Technical Specification document which details the changes you'll need to make."

REMINDER: MANDATORY CHANGES ON MASTERCARD AUTHORISATIONS

To help improve the accuracy of cardholders' available funds on debit and credit cards as well as addressing regulatory concerns regarding the use of Pre-Authorisations, MasterCard has mandated a number of changes to how authorisations are processed.

Since **1st October 2014**, all MasterCard authorisations must be defined as either a 'Final Authorisation' or a 'Pre-Authorisation' and also flow the SRD. These changes apply to all transactions made on the following MasterCard brands: MasterCard Credit, MasterCard Debit, Maestro Debit and Maestro International.

NEXT

FINAL AUTHORISATIONS

Final Authorisations are used in most face to face environments, where goods or services can be dispatched and settled within four business days of the original authorisation. A Final Authorisation is categorised as:

- An authorisation on a transaction (greater than zero) for the final or known amount.
- The transaction may no longer be cancelled after the authorisation is requested other than by performing a refund. This excludes any technical failures before the transaction completes.
- The transaction must be cleared (sent to the card processor) within four business days of the authorisation date.

PROCESSING INTEGRITY FEE (PIF) AND UNKNOWN FINALITY FEE (UFF)

An authorisation marked as a Final Authorisation that doesn't meet the above criteria, for example, you don't send your transactions to us within four days, will attract a PIF of 0.25% (minimum 3p) of the transaction value. This is in addition to the service charge applied to the transaction. Similarly, transactions not flagged as Final Authorisation that fall into the qualifying criteria above will attract a 1p UFF. To avoid either of these fees being applied, it's vital you select the correct authorisation type for the transaction you are undertaking.

PREV

PRE-AUTHORISATIONS AND WHEN THEY SHOULD BE USED

Pre-Authorisations are used when the goods or services cannot be dispatched or delivered within four business days and anywhere that the final amount of the transaction may not be known at the point of original authorisation. For example, an online business that isn't able to fulfil an order in a single transaction. These transactions will attract a payment guarantee period of up to 30 days (please note that all Maestro card authorisations only have a payment guarantee period of seven days). A payment guarantee period is the length of time that an authorisation request holds funds in a cardholder's account, it doesn't confirm the cardholder's identity or guarantee payment. Any transaction processed outside of these timescales requires another authorisation.

A pre-authorisation is categorised by any of the following characteristics:

- An authorisation for an 'estimated' amount (greater than zero).
- Where a transaction isn't cleared (sent to Global Payments to debit the cardholder) within four business days of the original authorisation date.
- Where a payment guarantee period is required for up to 30 days. For example, online orders where it is not clear at the point of sale when goods will be dispatched.
- Where the cardholder will be offered the option to pay by an alternate means at completion. For example, an hotelier may hold a room open for a period of time against an authorisation code but may offer the customer the choice to 'checkout' by paying cash.

If you're unsure whether your Global Payments terminal(s) can perform a Pre-Authorisation and want to check, please call our helpdesk on **0345 702 3344*** selecting the option for 'all other enquiries'.

It's your responsibility to ensure you select the correct type of authorisation for the transaction you're carrying out. Failure to define an authorisation as either a Final Authorisation or a Pre-Authorisation could result in charges being levied by MasterCard, for which you'll be liable.

"Transactions will attract a payment guarantee period of up to 30 days."

NEXT

PRE-AUTHORISATION FEE (PAF)

Where you select to perform a Pre-Authorisation, a PAF of 0.02% (minimum 1p) of the authorisation value will be applied in addition to the service charges applied to the transaction.

FINALISING PRE-AUTHORISATIONS AND FLOWING SRD

When you're ready to complete a Pre-Authorisation, a clearing[1] record must be created that contains the SRD (see Reminder: Mandatory Changes – Scheme Reference Data (SRD) section on previous page) from the Pre-Authorisation(s), the authorisation code from the first Pre-Authorisation and the actual transaction value. The clearing record may relate to a single Pre-Authorisation, or a Pre-Authorisation and several incremental authorisations.

If the value of the clearing record is greater than the total value of any Pre-Authorisation plus any incremental authorisation(s), a further incremental authorisation must be performed for the difference to ensure the value of the clearing record is equal to the total value of the Pre-Authorisation and any Incremental Authorisations.

MASTERCARD AUTHORISATION REVERSALS

We've updated the way we process reversals and the way they are matched to the original transaction data. This is to reduce the number of reversals that can't be matched online due to the original data not being found or verified, whilst still preventing fraud caused by submitting bogus, repeat or high value reversal messages.

There are a number of situations where a reversal may be required, these include:

- Undoing a transaction that has been processed in error.
- The transaction is not completed in full or the final amount is less than the authorised value.
- The card processor can reasonably infer that a transaction did not complete correctly.

These changes will assist customers who trade in the Travel and Entertainment sector or online and who process they do not immediately follow the original authorisation.

If you have any questions about these mandatory changes, please call us on **0345 702 3344*** selecting the option for 'all other enquiries'.

[1]Clearing is where the merchant (you) sends all their card sales transactions to their processor (Global Payments) for that day. If you have a physical card terminal, this usually happens when you complete your end of day banking.

*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

PREV

"We've updated the way we process reversals and the way they are matched to the original transaction data."

NEXT

PROCEDURAL UPDATES

HOW TO PROCESS FALLBACK PAPER VOUCHERS

If there's a problem with your terminal, your telephone line or power supply, you may need to use fallback paper vouchers to accept a card payment. Here's a brief guide to the steps you must follow if you need to do this.

Remember you can find more detailed instructions on paper vouchers in the 'Using Fallback Paper Vouchers' section of your *Merchant Operating Instructions.*

- Ensure your merchant plate is securely tightened to the imprinter.
- Undertake validation checks on the card as detailed in your *Merchant Operating Instructions.*
- Place the customer's card on the imprinter base. **Please remember, it's not possible to process Maestro, Visa Electron, V PAY, Discover Global Network or UnionPay cards or Mobile POS Solution transactions using paper vouchers.**
- Position the paper voucher over the merchant plate and the customer's card.
- Push the imprinter handle quickly and firmly to the right and then pull it back to the left so it sits in its original position. This imprints the card and merchant plate information onto the voucher.
- Fully complete the fields on the voucher using a black ballpoint pen and provide details of the goods/services purchased.
- Once you've completed the voucher, hand it to the cardholder for them to sign it. Check the signature against the one on the back of the card.
- All fallback transactions must be authorised. To do this call our authorisation centre on **0345 770 0600**. Lines are open 24 hours, 7 days a week, 365 days a year.
- Once you've obtained authorisation, write the code on the voucher. When you've done this, pass your customer the 'cardholder copy' of the voucher and their card. Retain the 'merchant copy' for your records. You must retain this securely for 5 years. See below for what to do with the 'process copy'.

"If there's a problem with your terminal, your telephone line or power supply, you may need to use fallback paper vouchers to accept a card payment."

WHAT HAPPENS NEXT

Complete a summary voucher and securely send this to us, together with all the process copies of your sales/refund vouchers, at the Freepost address below. Every batch of vouchers must be posted before the end of the third working day following the transactions.

Freepost RSGY-GYLY-GGEA
Global Payments
De Montfort Business Centre
51 De Montfort Street
Leicester
LE1 7BB

Remember not following the steps above closely could mean delays in processing your transactions or your transactions not being processed at all.

DO	DON'T
Call our authorisation centre	Duplicate vouchers
Securely place items on the imprinter	Write illegibly on the voucher
Firmly press on the handle when making the imprint	Hang on to vouchers. Send them to us as soon as possible
Remove the paper voucher first, then remove the credit card	Post paper vouchers to us unsecurely
Ensure the date, amount and signature are clearly written	Store paper vouchers unsecurely

If you have any queries about how to process paper vouchers, please call us on **0345 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open, Monday to Friday, 9am – 6pm, excluding public holidays. To helps 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 0345 602 4818.

NEXT

CHANGES TO YOUR TERMINAL'S END OF DAY PROCEDURE

We're making a change to our infrastructure that processes your card transactions. Part of this involves the route that your transactions take in order to be processed by us, which will give us greater control of the processing cycle.

We'll keep the impact of these changes to a minimum, however, one of the changes we're making is to the time that we batch together your transactions and submit them for processing. Previously, the deadline to complete your End Of Day banking was 4.00am daily. This time has had to change to 2.00am so that your card transactions can be credited to your bank account within the same timescales as they currently do.

Please note that the 2.00am deadline already appears in the latest version of your *Merchant Operating Instructions* (dated 08/2015) so you may already be aware of this new time.

AUTOMATIC END OF DAY

We're aware that some of our customers have an Automatic End Of Day procedure set up on their terminal that may run after 2.00am. We'll write to those customer that are impacted shortly to let you know what changes you'll need to make.

If you have any queries regarding this change, please call us on **0345 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open, Monday to Friday, 9am – 6pm, excluding public holidays. To helps 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 0345 602 4818.

DO YOU TRADE ONLINE?

CHARGEBACKS RELATING TO TERMS AND CONDITIONS, CANCELLATION/RETURN/ REFUND POLICY AND PROPER DISCLOSURE

If you do and you want to impose specific terms and conditions to your transactions, Visa and MasterCard require these to be properly disclosed and agreed to, by the cardholder, prior to completion of their transaction.

Visa and MasterCard also require you to include a cancellation/return/refund policy on your website and this too should be properly disclosed and agreed to, by the cardholder, prior to them completing their transaction.

To defend chargebacks relating to disputes over imposed terms and conditions or where a cardholder cancelled an online order and the merchant refused to refund, we are required to prove proper disclosure of the cancellation/ return/refund policy. To enable us to do this, you'll need to provide us with the following as part of any chargeback:

- Evidence that, as part of the sequence of web pages accessed by the cardholder prior to checkout, the merchant included a 'click to accept' button or another type of acknowledgement showing the cardholder agreed to the terms and conditions and cancellation/return/refund policy, and
- details of the terms and conditions and cancellation/return/refund policy disclosed to the cardholder as part of this acceptance.

If you have any queries regarding this, please call us on **0345 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open, Monday to Friday, 9am – 6pm, excluding public holidays. To helps 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 0345 602 4818.

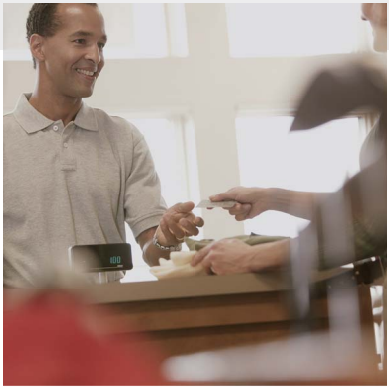
"Visa and MasterCard also require you to include a cancellation/return/refund policy on your website"

NEXT

RETAIL SPECIFIC NEWS UPDATE

The following Retail Specific section contains updates from the Card Schemes that you need to apply if you own your own Point of Sale (PoS) equipment, rent card terminals from a supplier other than Global Payments or use a Payment Service Provider (PSP) to accept card payments on the internet.

If you rent a card terminal from us or use Global Iris to accept card payments on the internet, these updates will be made automatically and no action is required by you and you don't need to read any further.

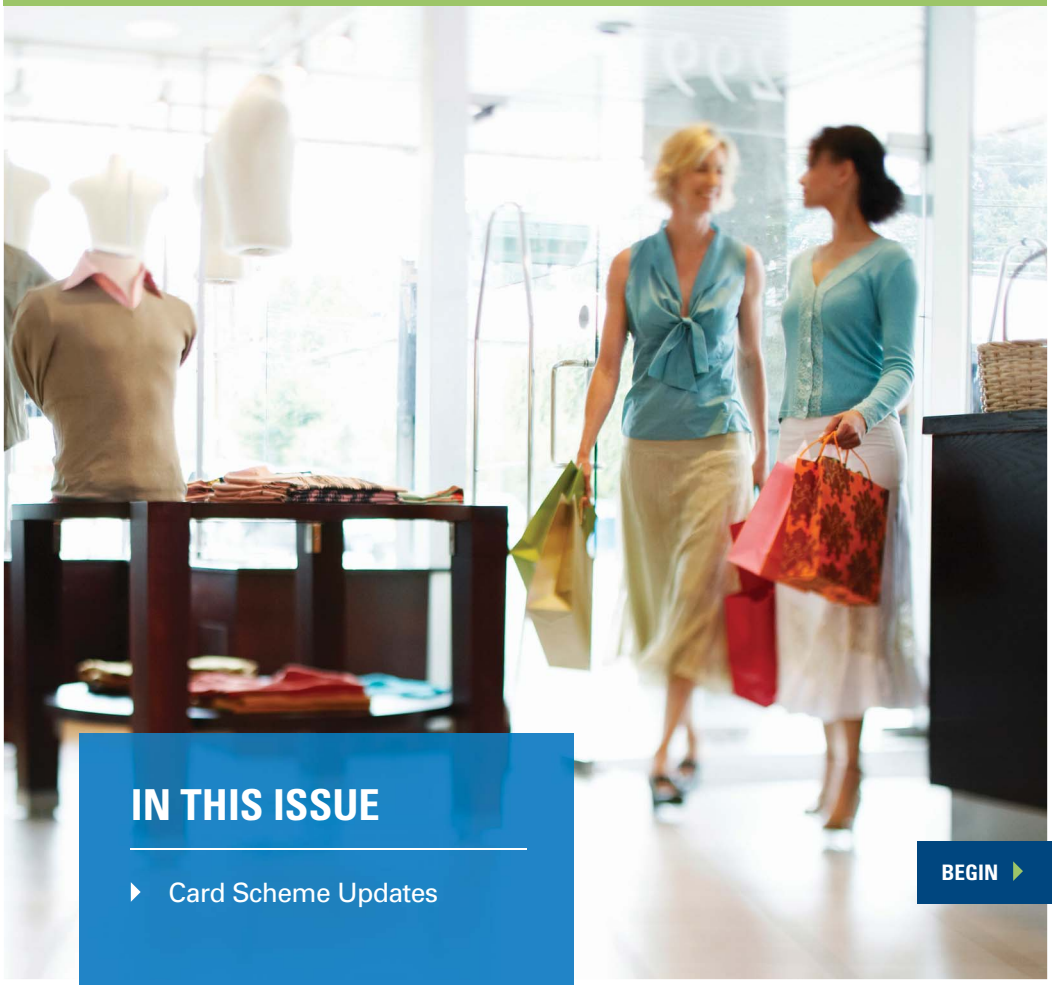


globalpayments

SPRING 2016

RETAIL SPECIFIC NEWS

INTERACTIVE EDITION - KEEPING YOU IN THE KNOW



IN THIS ISSUE

BEGIN

CARD SCHEME UPDATES

DEPLOYMENT OF CONTACTLESS CAPABLE TERMINALS

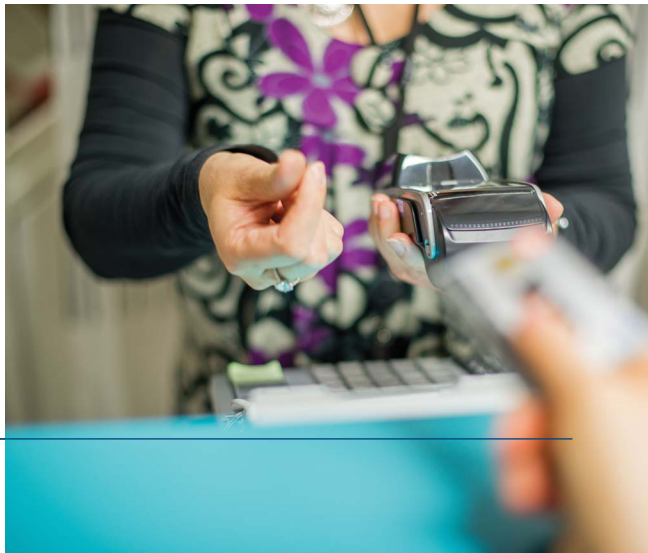
Visa has mandated that from **1st January 2016** any new terminal must be Contactless capable. This means if you're opening a new outlet or simply adding an additional terminal in an existing outlet, any new terminals that you place must support Contactless payments. Where an existing terminal is faulty and needs to be replaced, this can be done on a like for like basis and doesn't need to be replaced by a Contactless capable device.

Currently there isn't a need to replace existing terminals that don't support Contactless payments with ones that do. But, when you're considering buying new terminals, please be mindful of this mandate and the fact the Card Schemes are looking for all terminals to support Contactless payments by the end of 2019.

If you have any queries regarding this, please call us on **0345 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open between 9am - 6pm Monday to Friday, excluding public holidays. To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide a Textphone service on 0345 602 4818.

"...if you're opening a new outlet any new terminals that you place must support Contactless payments."



NEW MASTERCARD BIN RANGE

MasterCard has announced that from **14th October 2016** they're introducing a new series of Bank Identification Numbers (BINs) that begin with a '2' in addition to their current range The new '2' series BINs will be processed the same way as MasterCard's existing BIN range that's between "51–55". Support of the new BIN range is mandatory for **all businesses**.

The table below contains both the existing and new MasterCard BIN ranges:

CARD BRAND NAME	LOWEST BIN NO	HIGHEST BIN NO	CARD NO LENGTH
MasterCard (Current)	51000000	55999999	16-19 Digits
MasterCard (New)	22210000	27209999	16-19 Digits

Supporting the new BIN range will protect you from loss of business due to being unable to accept transactions from cardholders that have cards issued in the new BIN range. It'll also help prevent you from receiving any operational fines for not being able to accept the new cards.

If you own your own terminals, rent them from a third party or use a Payment Service Provider to accept payments online, you'll need to contact your supplier to get them to upgrade your equipment so you can accept the new cards. If you rent a terminal from us, or use our Global Iris service to accept payments online, you don't need to do anything as we'll automatically update it before the change comes into effect.

If you have any queries regarding MasterCard's new BIN ranges, please call us on **0345 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open between 9am - 6pm Monday to Friday, excluding public holidays. To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide a Textphone service on 0345 602 4818.

NEXT

ANNUAL REVIEW OF PUBLIC KEYS

All credit and debit cards that contain a chip rely on public keys to authenticate the card as being valid and to perform offline enciphered PIN verification. These keys are reviewed annually to ensure they've not been compromised and still offer adequate protection to both you, the merchant, and your customers.

This year's review has just taken place and to comply with this, the public keys listed below must be loaded into Point of Sale terminals with immediate effect:

- 1152 bit public key with an expiration date of no later than **31st December 2017.**
- 1048 bit public key with an expiration date of no later than **31st December 2024.**
- 1984 bit public key with an expiration date of no later than **31st December 2025.**

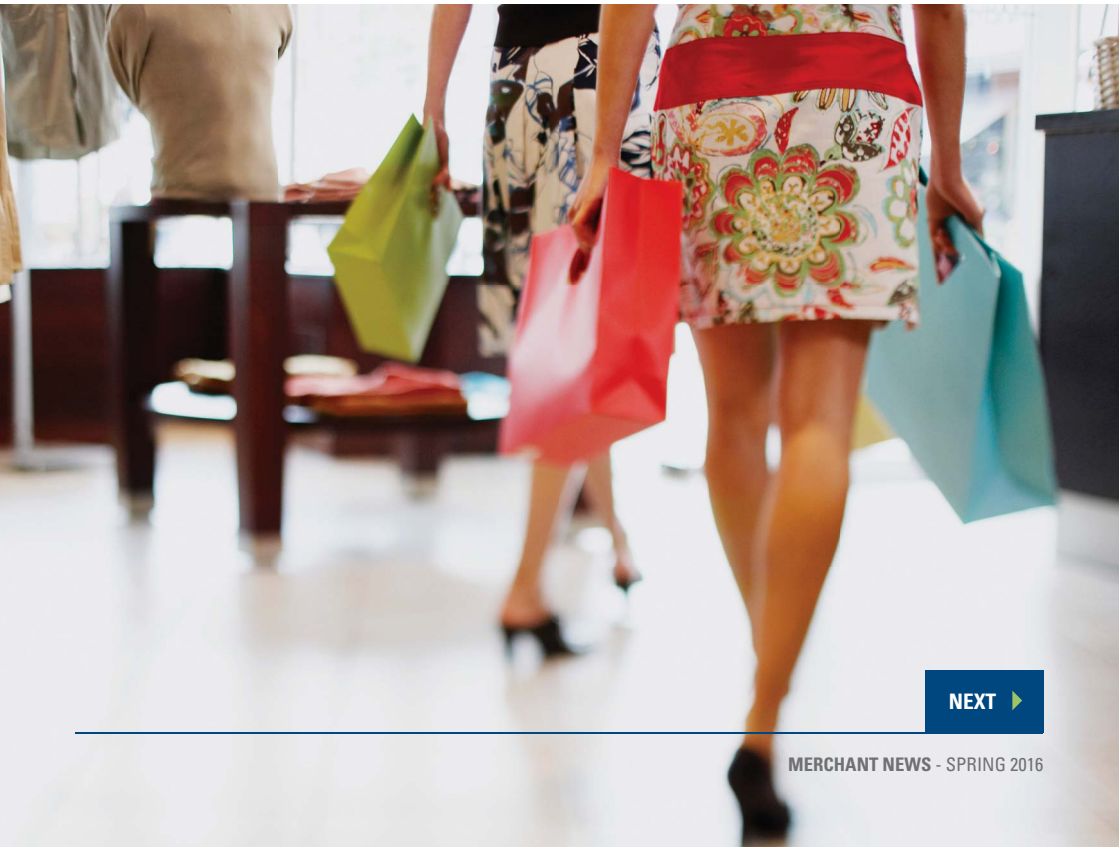
If you own your terminals or rent from a third party, you'll need to contact your supplier to request they update your terminal to meet the mandate. Failure to do so may lead to card acceptance problems and fines being imposed by the Card Schemes.

If you rent a terminal from us, you won't need to do anything as we'll automatically update it over the next few months so you comply with the mandate.

If you've got any queries regarding Public Keys, please call us on **0345 702 3344*** selecting the option for 'all other enquiries'.

*Lines are open between 9am - 6pm Monday to Friday, excluding public holidays. To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide a Textphone service on 0345 602 4818.

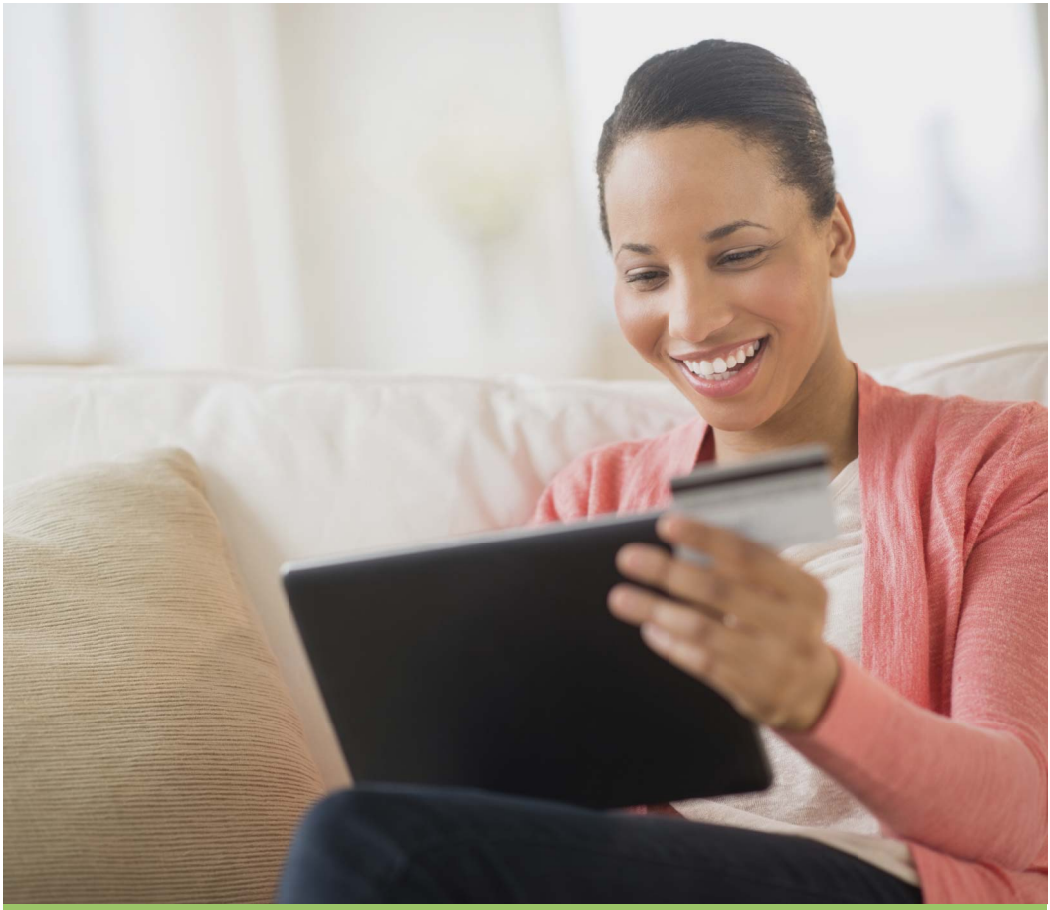
"If you own your terminals or rent from a third party, you'll need to contact your supplier to request they update your terminal to meet the mandate."



NEXT

globalpayments

HOME PAGE



SERVICE. DRIVEN. COMMERCE

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.

GP373