globalpayments

AUTUMN 2016

# MERCHANT NEWS

**INTERACTIVE EDITION** - KEEPING YOU IN THE KNOW


## IN THIS ISSUE



BEGIN

# WELCOME TO THE AUTUMN 2016 EDITION OF MERCHANT NEWS

In this latest edition of Merchant News, in addition to our usual features on Card Industry News, Product News and Card Scheme Updates, you'll find out more about Realex Payments. They've been a division of Global Payments since March 2015, but we've been partners since 2012, as they've been providing our ecommerce platform, Global Iris. Online spending accounted for 24 per cent* of total card spending in May 2016, up from 22 per cent in May 2015. In total for May, online spending accounted for £12.6 billion, an increase of £115 million. So if you think that being able to accept payments online could benefit your business, make sure you find out more about Realex Payments.

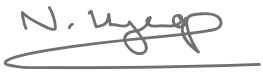
You'll also see an article on the different ways you can accept Contactless payments on your Global Payments terminal. These now account for eighteen per cent* of all card purchases compared to seven per cent in May 2015. Consumer spending on Contactless cards in the first half of 2016 outstripped Contactless spending for the whole of 2015**. So it's important you're aware of the different ways your customers could try and pay for their purchases in-store, for example with a key fob, sticker, watch or mobile phone.

We're also supporting Financial Fraud Action UK's (FFA UK) 'Take Five To Stop Fraud' campaign, which launched in the middle of September. You can find more details on the campaign, together with how we're supporting it, by reading on.

At Global Payments, not only are we a card processor, we're deeply involved in our local community. Back in May, a team of 20 employees known as the 'Global Peddlers', took part in the Tour de Leicestershire riding 175 miles around the county in two days. This was the climax to a year of fundraising by all our staff to support LOROS, a Leicester based charity who provide free, high quality compassionate care for terminally ill patients, their families and carers. Joined by our Chief Executive Officer from our head office in Atlanta, Jeff Sloan, the peddlers raised over £33,000, which went towards a final donation of nearly £45,000 to LOROS. You can read more about the peddlers on page 4 of this edition of Merchant News.

We've also sponsored the Overcoming Hardship category at this year's Heroes of Leicestershire Awards. This category struck a chord as many of us have known someone that has personally overcome hardship, whether adversity, illness or disability. It was a real honour to be able to present the winner Pam Hunt, who has shown tremendous resilience, with her award, as well as meeting the other finalists in the category.

All the best



**Nigel Hyslop**
**President and Managing Director UK**

*UK Cards Association – UK Card Expenditure Statistics: May 2016
**UK Cards Association – UK Card Expenditure Statistics: June 2016

NEXT

# GLOBAL PEDDLERS

## TOUR DE LEICESTERSHIRE 2016

In his introduction, Nigel Hyslop let you know about the Global Peddlers and their fund-raising for LOROS, a Leicester based charity who provide free, high quality compassionate care for terminally ill patients, their families and carers. We're pleased to be able to share more of their story with you.

The Tour De Leicestershire was our third company-organised cycling event, which this year saw us being joined by colleagues from Realex Payments, as we rode 175 miles over two days. Unlike previous years, which had enjoyed good cycling conditions, this year saw all the different types of weather that early summer in the UK can throw at a cyclist.

Setting off from our Leicester office at 8:30am on the first morning, we hit the rain as soon as we reached the first notable hill of the ride. This set the pattern for the rest of day one! We dodged in and out of the rain until the weather eased up somewhat late morning, when we arrived for lunch at the LOROS shop in Oakham. We took a loop around the beautiful scenery of Rutland Water, where at mile 70, the rain really started to come down. Trekking back through the north Leicestershire countryside, the rain made the terrain and road surfaces exceptionally challenging, but we finally rolled back into Leicester just before 7:00pm.


LOROS
Hospice Care for Leicester, Leicestershire & Rutland

PREV

Day two was a much more agreeable affair; the sun was shining, which brought out the real beauty of the English countryside. Our 75 mile ride took us around south Leicestershire, and once again we met the LOROS team at their Market Harborough shop. We negotiated our way through several plates of cookies and flapjacks before heading back to Leicester via some sharp hills, none of which our legs were particularly pleased to find in the last 25 miles of the ride! We arrived back at the Leicester office to a rapturous welcome from our colleagues and LOROS representatives just after 3:30pm.

The Peddlers 2016 Role of Honour went to Jeff Sloan, Ian Webb, Phil Jones, Lynda Broughal, Gary Conroy, Andy Cope, Daniel Devitt, Liliana Fernandez, Murilo Goulart, Mark Johnson, Gary Lee, Coral McCallum, Andra Milender, Dave Moore, Valerie O'Mahoney, Joe Perry, Pete Preocanin, Gearoid Quigley, Jamie Snashall, and Donovan Stenning. Thanks also goes to our ever present support team of John Sutton, Janet Beeson and Ange Halford for their exceptionally appreciated support work too. Seeing their smiling faces when our bodies were starting to stiffen and suffer, and we were in need of refuelling, really made a difference. We'd also like to thank Ingenico and Fexco for their generous support in sponsoring the peddlers cycling jerseys, together with Travelodge for their assistance in providing them with their overnight accommodation on the ride as well.

NEXT


# INTRODUCING REALEX PAYMENTS

## GLOBAL IRIS IS CHANGING

If you haven't heard of Realex Payments before now, that's all set to change. They became a division of Global Payments in 2015, but our relationship goes back further than that. They've been partnering with us since 2012, providing over 5,000 of our customers in the UK with Global Iris, the ecommerce platform which Realex developed for us.

As we continue to integrate Realex into the Global Payments family, we're taking the opportunity to transition existing customers from Global Iris to the full Realex ecommerce Platform. New Global Iris customers, who've joined us since 4th July 2016, have automatically been onboarded onto the Realex Ecommerce Platform. Existing Global Iris customers will be migrated over to this in the near future and we'll be contacting you shortly, to let you know more information about this.

This rebrand cements Realex Payments as part of our business. It also means that all of our customers will be able to take full advantage of the complete feature rich solution from this well-established ecommerce platform provider.

PREV

**Existing Global Iris customers will now have access to many additional benefits including:**

### PRODUCT RELEASES

- Instant access to the latest product feature releases such as a large number of upcoming additional alternative payment methods.

### HOSTED CHECKOUT SOLUTION WITH CARD MANAGEMENT

- A fully customisable, mobile optimised Hosted Payment Page, which allows your customers to manage and store their cards of choice and a simple, secure check-out experience.

### FRAUD MANAGEMENT

- New Queue Management feature; you can now hold and review transactions before approval.
- Access the completely revamped fraud engine, providing you with better transaction visibility and more control.
- Realex Payments' partnership with CyberSource delivers an industry-leading enterprise fraud solution, which applies over 260 separate fraud checks on your transactions, powered by intelligence extracted from 68 billion transactions processed every year through Visa Inc.

### TRANSACTION REPORTING

- Real Control reporting tool that provides you with an intuitive dashboard, displaying all key information including all processed and held transactions for review.

### DEVELOPER HUB

- Everything a developer needs to integrate Realex Payments including Android and iOS libraries, software development kits (SDKs), sample code and test accounts for all commonly used languages.

We're excited to be working with new and existing customers and introducing you to the benefits of selling online with the Realex Ecommerce Platform, which includes a powerful payments solution, expert and dedicated customer service, including unique knowledge and insights into the ecommerce and mobile landscape.

Best regards

**Dave Willis**

Head Of Sales
Worldwide Ecommerce

**Dave Willis -** Head Of Sales Worldwide Ecommerce

**"We're excited to be working with new and existing customers and introducing you to the benefits of selling online with the Realex Ecommerce Platform"**

NEXT

**“For shoppers buying online, we provide a seamless checkout experience across any device with a wide range of payment methods”**

## A WINNING TEAM – GLOBAL PAYMENTS AND REALEX PAYMENTS

Realex Payments currently processes €35bn ecommerce transactions annually, while working with some of the world's leading brands, who rely on us to deliver a secure, reliable and innovation payment solution. The combination of our card processing capability and Realex Payments' Hosted Checkout Solution has created a truly winning solution for both large and small online merchants.

### HOW REALEX PAYMENTS HELP BUSINESSES TO SELL ONLINE

For businesses selling online, we can provide you with everything you need to get up and running. And as you grow in scale, both locally and globally, we can help you to continually optimise your payment conversion and acceptance. For shoppers buying online, we provide a seamless checkout experience across any device with a wide range of payment methods.

### A COMPLETE SOLUTION FOR SELLING ONLINE

*According to a recent report from the UK Cards Association, £210 billion was spent online in 2015, representing 32% of all total card spending in the UK with mobile ecommerce representing 51% of this figure.*

While opportunities for online businesses are plentiful, consumers also have become increasingly discerning when it comes to buying online and you need to deliver a smooth payments experience across any device. The slightest delay or complication in your payment page loading can directly lead to an increase in abandoned sales.

Our Hosted Checkout Solution can help you increase your conversion and acceptance rates with a frictionless payment experience, removing overheads associated with Payment Card Industry Data Security Standard compliance and allows for card storage and Dynamic Currency Conversion (DCC) capabilities. It's also been optimised for mobile devices, automatically resizing to suit individual screen sizes.

We also provide native Android and iOS libraries, so developers can easily incorporate our Hosted Payment Page in their app. If this captures card data, these also provide a suite of checks to validate the card data before it's submitted to us. We've also extended support for Apple Pay and intend on providing support for Android Pay and Samsung Pay in the near future.

### TRUSTPILOT

Realex Payments strive to ensure that all our customers experience world class customer service combined with a powerful and reliable payments solution. Our team is dedicated to helping you and there's always someone on the other end of a phone or email to help you and offer expert service.

This dedication to reliable, expert customer service is reflected in our TrustPilot score.

To find out more about how we can help your online business, visit the Realex Payments website at **www.realexpayments.com** or call them on **+44 (0)203 650 6000***.

*Lines are open between 8.30am – 5.30pm 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

# PRODUCT NEWS

## CONTACTLESS PAYMENTS

**Contactless has become a key payment method in the last year. It's fast, easy and secure. There's been a growth in the different ways Contactless transactions can be made, and understanding these will help your customers pay effortlessly.**

### PASSIVE CONTACTLESS: CONTACTLESS CARDS, STICKERS, WRISTBANDS OR FOBS

Contactless transactions started with credit and debit cards and these are still the main form of payment, where the card communicates with a Contactless reader to make a payment of up to £30. More recently, Contactless technology has been embedded in stickers, wristbands, key fobs and even jewellery and clothing, which can then be used to make Contactless payments.

Cardholder has a Contactless enabled card or product (e.g. wristband or key fob) with an embedded antenna or chip that communicates securely with a Contactless reader.


Accept a Contactless transaction by the cardholder tapping their Contactless card or product on your Contactless reader, to securely transfer data. The cardholder does not need to use any verification, e.g. PIN. **Transaction Limit £30.**

Your card terminal will give a confirmation sound and message to show the transaction is complete. A cardholder receipt is optional and should be supplied if the cardholder asks for it.


Contactless transactions are secure, offering the same protection as chip and PIN transactions. Liability is with the issuing bank in the event of fraud.

## ACTIVE CONTACTLESS: MOBILE WALLETS

Credit or debit card[1] details can be securely stored on a smartphone app (for example Apple Pay or Android Pay) and then used to make a Contactless payment either with the phone or a compatible smart-watch. A chip in the device communicates with the Contactless card reader to make the payment. These differ from Contactless payments made with a card, because the transaction is always authorised by the cardholder identifying themselves on their device, usually with a fingerprint or the PIN they use to unlock their device. The £30 Contactless limit doesn't apply to these transactions, as mobile wallets support 'High Value Payments' Contactless card payments above £30.

If you rent a terminal from us, then you're already set-up to accept High Value Payments (HVP). If you own your own terminal or rent them from a third party, you need to ensure your terminals meet the required certification levels and have the HVP functionality switched on.

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

[1]A card doesn't have to be Contactless to be loaded into a mobile wallet and used for a Contactless payment, as it's the mobile device that carries out the Contactless communication not the card.

[2]BarclayCard Contactless Mobile has a £100 limit imposed by Barclays. Apple Pay and Android Pay have no limit.

*Lines are open between 9.00am – 6.00pm 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.

Cardholder has a Contactless enabled device (smartphone / watch) with their card payment details securely stored.


Accept a Contactless transaction by the cardholder tapping their device on a Contactless reader and verifying themselves on their device, e.g. by fingerprint or device PIN. **There's No transaction limit.**[2]


Your card terminal will give a confirmation sound and message to show the transaction is complete. The cardholder's phone will beep / vibrate and show confirmation on screen. A receipt is optional and should be supplied if the cardholder requests one. The cardholder's phone also shows them a list of transactions.


Contactless mobile wallet transactions are secure, offering the same level of protection as chip and PIN, including for transactions above £30, as long as the transaction has authorised successfully and been verified by the cardholder on their device. In the event of fraud the liability is with the card issuer.

NEXT

# SPOTLIGHT ON CORPORATE SOCIAL RESPONSIBILITY: MAKING PENNIES COUNT

Global Payments is proud to have enabled Pennies, the digital charity box, in a variety of our customers since 2013. Together we make it possible for consumers to donate small, ad hoc amounts to charity – by rounding or topping up their bill when paying by card.

Pennies makes giving to charity easy, anonymous and affordable. It's the digital upgrade of the traditional charity box, designed to fit in with consumers' increasingly cashless lifestyles. It also resonates with the public's growing reticence to give up their data with their donation, as neither Pennies nor the merchant captures any personal information and there's no follow up.

Our customers, Warwick Castle, Yorkshire Wildlife Park and the National Sea Life Centre, and the veterinary practice Medivet, all use Pennies to raise money for their chosen charities (respectively The Merlin Magic Wand Children's Charity, Yorkshire Wildlife Park Foundation, Sea Life Trust and The Wilderness Foundation). In just two and a half years, these merchants have made consumers' pennies count for charity to the tune of £120,000 from more than 245,000 individual customer 'micro-donations'.


# ANK OU

Pennies!
The digital charity box

NEXT

**"Niki Akhurst, Director of Business Development at Pennies said: 'Global Payments has unlocked £120,000 for charity so far"**

## CASE STUDY

In the last year, 200,000 generous clients have helped Medivet reach a milestone of £100,000 through Pennies - enabled by Global Payments; which is being used to fund efforts being made to protect the rhino in South Africa.

The veterinary group, which has over 130 practices in the UK, launched their Medivet Saving the Rhino campaign with the Wilderness Foundation and former colleague, Dr William Fowlds, in May 2015.

Medivet affords clients the chance to raise funds by electing to add a 50p donation to their bill at most Medivet practices.

John Smithers, Medivet Senior Partner and co-ordinator of the Medivet Saving the Rhino campaign, said: "We're absolutely delighted with the response from our clients and I wish to thank them for their kindness and support. Importantly, our clients are also helping raise awareness of the crisis amongst the communities we serve and inspire people to get involved in the worldwide campaign to stop wildlife crime."

In 2014, over 1,200 rhinos were poached for their horns in South Africa, making it the worst poaching year on record. In 2015 there was a slight decline taking the number down to 1,175 and, although this is a positive step, Medivet and the Wilderness Foundation say more rhinos are being killed than are being born, so more needs to be done to help save them.

Niki Akhurst, Director of Business Development at Pennies said: 'Global Payments has unlocked £120,000 for charity so far, by enabling Pennies in the theme park/entertainment market – and

the veterinary sector through Medivet. We've been able to demonstrate that consumers enjoy 'feel-good' giving when purchasing goods and services for their family - and beloved pets. By giving the public's small change a big purpose, Pennies and Global Payments have translated thousands of digital clicks of generosity into tangible social impact both domestically, and internationally.'

Launched in late 2010, by July 2016 Fintech non-profit Pennies – a charity itself - had generated over 30 million donations and raised £7 million for merchants' nominated charities (exceeding 120). For more information about Pennies and its work, visit **www.pennies.org.uk**.

If you would like to use Pennies in your business to support charity, please call us on **0345 702 3344***, selecting the option for option for 'all other enquiries'.

*Lines are open between 9.00am – 6.00pm 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

# HOMECURRENCYPAY ON VERIFONE TERMINALS

It's been just over 18 months since we launched HomeCurrencyPay, our own Dynamic Currency Conversion (DCC) service, onto our Ingenico terminals. Since it launched we've processed over 1.5 million DCC transactions.

HomeCurrencyPay offers you the ability to provide your international customers with the choice and convenience of paying for goods and/or services in their own home currency. It also credits your account in sterling for easy reconciliation, while your customer's sales receipt reflects their payment in both their home currency and sterling. There's no additional charge for this service, in fact it gives you the opportunity to earn commission as a percentage of each HomeCurrencyPay transaction you submit. Any commission earned will be reflected as a credit on your monthly invoice.

We've recently written to eligible customers who rent VeriFone terminals from us, to let you know that we'll be upgrading your terminal with HomeCurrencyPay. This will allow even more of you the opportunity to offer your international customers the ability to pay for purchases in their home currency or sterling. The upgrade will take place over the coming weeks as part of your terminal's regular maintenance call. So you'll experience a seamless implementation and the ability to provide instant conversion of all the major currencies on the terminal.

If you have any queries regarding HomeCurrencyPay, or if you rent a terminal from us and think it could benefit your business, please call us on **0345 702 3344***, selecting the option for 'all other enquiries'.

*Lines are open between 9.00am – 6.00pm 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.

HomeCurrencyPay

**"There's no additional charge for this service, in fact it gives you the opportunity to earn commission as a percentage of each HomeCurrencyPay transaction you submit."**

NEXT


# TAKE FIVE TO STOP FRAUD

Banks and financial service providers work hard to protect their customers – in the UK last year, their innovative systems stopped 70% of attempted fraud from actually happening. The 30% that did happen though? That cost the nation £755 million.

Clearly, something needs to be done, and Financial Fraud Action UK (FFA UK) doesn't believe this 'thing' has to be complicated. In fact, it can be as simple as encouraging people to take a moment to stop and think.

Many people may already know the dos and don'ts of financial fraud – that no-one should ever ask them for their PIN number or full password, or ever make them feel pressured into making a decision. The trouble is, in the heat of the moment, it's easy to forget this.

After all, trusting people on their word is something everyone tends to do instinctively. Until we have good reason not to. If someone says they're from your bank or another trusted organisation, why wouldn't you believe them?

Before you take their word for it though, Take Five, a new campaign led by FFA UK, urges you to stop and consider whether the situation is genuine – to stop and think if what you're being told really makes sense.

Take Five is created in collaboration with FFA UK's members (the nation's major banks, credit, debit and charge card issuers, and card processors), partners, (the Government, Cifas and the City of London Police) and most importantly, with you, the public.

**"Many people may already know the dos and don'ts of financial fraud – that no-one should ever ask them for their pin number or password, or ever make them feel pressured into making a decision. The trouble is, in the heat of the moment, it's easy to forget this."**

You can find more information by visiting the campaign's website at **https://takefive-stopfraud.org.uk/**

In support of the Take Five campaign, we've produced a number of guides to help businesses identify where fraudsters may try their luck. By visiting our website at **www.globalpaymentsinc.co.uk**, logging into the 'Customer Centre' using your Merchant ID and clicking on 'Card Processing' you can find and download copies of the following guides:

- Fraud Hints And Tips Guide
- Card Not Present Fraud Guide
- Fighting Fraud At Every Level

We hope they'll help you understand more about fraud and how you could stop this happening to you.

The FFA has also produced guides to help you both as a business and a consumer stay safe too. You can find out more by visiting their website: **https://www.financialfraudaction.org.uk/**

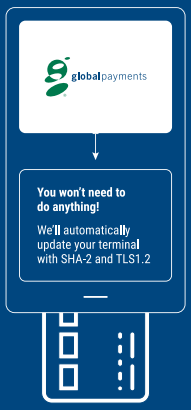
NEXT

# CARD INDUSTRY AND CARD SCHEME NEWS

## REPLACEMENT OF SHA-1 CERTIFICATE WITH SHA-2 CERTIFICATE AND SSL WITH TLS 1.2

### WHO PROVIDES YOUR PAYMENT TERMINAL?

**01.**




**02.**

**Own, Rent or use a Payment Service Provider (PSP)**

Contact your supplier to check that your terminal meets the SHA-2 Certification and the TLS 1.2 protocol.

**If Yes** – then you don't have to do anything else.

**If No** - You'll need to get your terminals updated as soon as possible!

**Deadline Dates:**

- SHA-1 to SHA-2 Certification Migration – **31st December 2016**.
- SSL3 to TLS 1.2 Protocol Migration – **30th June 2018.**

**WARNING:**

Your transactions could be declined if you do not make this change.

> **"The 1st January 2017 date is driven by Google, Microsoft, Mozilla and others, who have announced they will end trust for all SHA-1 SSL certificates on this date."**

PREV

## WHAT IS SHA-2 AND TLS 1.2?

**SHA-2** (Secure Hash Algorithm) is an improved and more secure means of protecting secure internet sites that's being adopted by all Internet Service Providers from 1st January 2017 and replaces SHA-1. It's part of what enables us to process card payments for you.

**TLS 1.2** (Transport Layer Security 1.2) is a newer and more advanced secure protocol. Like the SSL (Secure Sockets Layer) protocol that it's replacing, TLS 1.2 is used to establish a secure communications channel between computer systems in order to protect the confidentiality and integrity of information that passes between them.

## HOW DOES THIS AFFECT ME?

**This mandate is required for all IP terminals and internet activity and is not limited to card payment processing.**

The 1st January 2017 date is driven by Google, Microsoft, Mozilla and others, who have announced they will end trust for all SHA-1 SSL certificates on this date.

## WHAT DO I NEED TO DO?

If you rent your terminals* from us, or use Global Iris/Realex Ecommerce Platform to accept card payments on the internet, you won't need to do anything as we'll automatically update these over the coming months so that they're compliant with this vital requirement.

If you own your own Point of Sale (PoS) equipment, rent card terminals from a supplier other than us or use a Payment Service Provider (PSP) to accept card payments on the internet, you'll need to contact your supplier to check that your equipment meets the SHA-2 certification and the TLS 1.2 protocol. If they don't, you'll need to get your equipment updated with these protocols as soon as possible and by the industry deadlines, at the latest.

If you have any questions regarding this important change, we've produced a series of FAQ's, which you'll find at our website at: **www.globalpaymentsinc.co.uk.** If these don't answer your questions, please call us on **0345 702 3344**** selecting the option for 'all other enquiries'.

*You must keep your terminal plugged in and switched on overnight, and ensure that you complete your end of day, so that we can update the software to ensure it's compliant. Failure to do this will result in your terminal not having the latest software installed and impact your ability to accept and process card payments.

**We're open for card processing enquiries 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

# NEW MASTERCARD BIN RANGE REMINDER

In the Summer edition of Merchant News, we let you know that from **14th October** this year, MasterCard is introducing a new series of Bank Identification Numbers (BINs) that begin with a '2' in addition to their current range. There'll be no changes to the way you accept these new cards. If you rent a terminal from us, or use Global Iris/Realex Ecommerce Platform to accept payments online, you don't need to do anything as we'll automatically update it before the new cards start being issued.

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 |

If you own your own terminals, please make sure that you read the article on the new BIN range in the Retail News Section, which you'll find later in this edition. 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'.

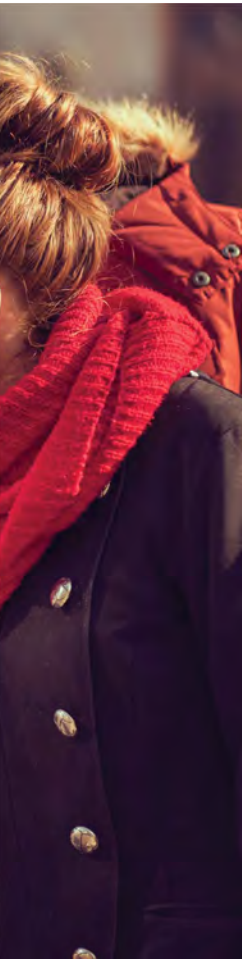
*Lines are open between 9am - 6pm Monday to Friday, excluding public holidays. To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide a Textphone service on 0345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

NEXT

# REMOVAL OF VISA'S REFERRAL SERVICE

Visa have advised that with immediate effect they'll no longer process transaction referrals on Card Present transactions. This means that any payments you accept on Visa credit and debit cards will now either be approved or declined, you won't be asked to call our authorisation service.

**For more information on the authorisation of card payments, please refer to your copy of our Merchant Operating Instructions.**



# DOWNGRADING OF MASTERCARD SECURECODE TRANSACTIONS WITHOUT ACCOUNT HOLDER AUTHENTICATION VALUE (AAV)

MasterCard have advised that any ecommerce transactions that are flagged as being authenticated by SecureCode, or where it's been attempted, but which don't include a valid AAV will be downgraded.

A downgraded transaction will attract a higher interchange rate and you won't benefit from the chargeback liability shift that SecureCode transactions attract. If you continue to submit transactions which are incorrectly flagged without a valid AAV, these may be automatically declined without being sent for authorisation.

If you've got any queries regarding AAV's and SecureCode, 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

# 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:

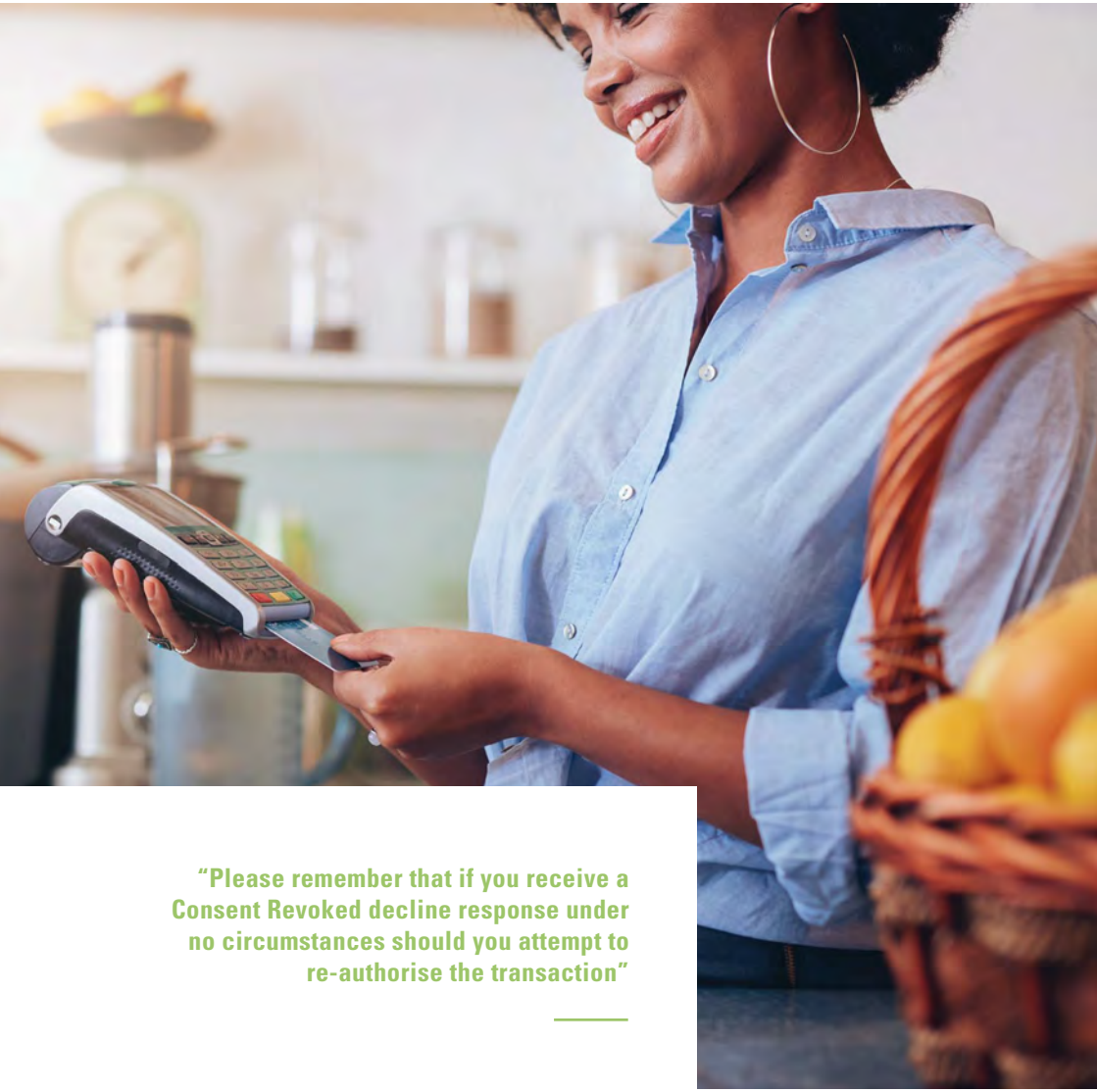
- Recurring Transactions
- Instalment Transactions
- Payday Loan Repayments

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'.

MasterCard and Visa 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.

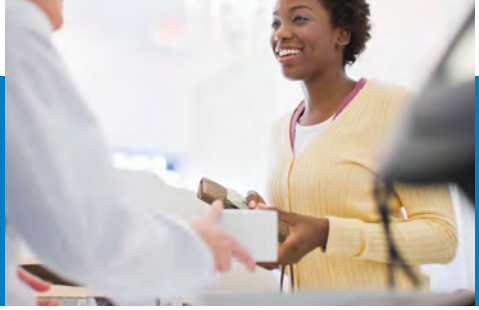
If you have any queries regarding this, please contact us on **0345 702 3344*** selecting the option for 'all other enquiries'.

*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.



**"Please remember that if you receive a Consent Revoked decline response under no circumstances should you attempt to re-authorise the transaction"**

NEXT



# PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

## PCI DSS VERSION 3.2 (V3.2) IS HERE!

You'll be aware that PCI DSS is a set of requirements issued by the PCI Security Standards Council (PCI SSC) for the protection of payment card data, which the Card Schemes (MasterCard and Visa) enforce. All our customers are required to achieve and validate their PCI DSS compliance to us.

V3.2 of the PCI DSS standard has been published and is now mandatory for all new validations and annual renewals from **1st November 2016.** Any new certifications received on or after this date under previous versions won't be accepted.

For customers that have achieved and evidenced their annual compliance to us on or before **31st October 2016**, your Self-Assessment Questionnaire (SAQ) or Report on Compliance (RoC) should still be valid* until your annual expiry date. When your compliance expires, you'll need to make your renewal against V3.2. However, to prevent any delays with your upcoming renewal we'd encourage you and anyone that handles or processes payment card data to begin the implementation of the new standard as soon as possible.

## WHAT'S NEW IN V3.2?

The release of V3.2 builds upon the release of V3.0 and V3.1 by including clarifications and additional guidance to existing requirements. These are updates to existing PCI DSS goals and requirements, which are intended to ensure organisations are addressing emerging threats and in particular, to ensure that service providers are fulfilling their responsibilities in providing services to others.

The new and amended requirements have had an impact to the size of the SAQs, specifically SAQ's A, A-EP and C-VT, which now have additional security requirements included. The reason for the increase in requirements under the scope of these SAQ's, is as a result of ecommerce websites and virtual terminals being increasingly targeted by hackers. Consequently, additional protection is now required for these merchant types.

We strongly recommend that you take the time to visit the PCI Security Standards Council website at: **https://www.pcisecuritystandards.org/index.php** for the full details of the new standard. Here you'll find lots of information and supporting documentation regarding the changes and general advice to help you achieve and maintain your PCI DSS compliance.

## NEXT STEPS…

For PCI Level 1 and Level 2 merchants, your compliance validation is likely to be through the submission of a RoC. Please contact your chosen Qualified Security Assessor (QSA) for any support or guidance on the new standard and how this will impact your next annual review.

For smaller Level 3 and Level 4 merchants who validate compliance through the completion of an SAQ:

- If you use Global Fortress to validate your PCI compliance to us, you'll be guided through this transition process, but you can contact SecurityMetrics directly on **0330 808 1003****.
- If you've not yet enrolled into Global Fortress and you need help in understanding your PCI DSS validation requirements, please call SecurityMetrics on **0330 808 1003****. Alternatively please visit **www.globalfortress.co.uk** where you can find out more about Global Fortress, or request one of their PCI consultants to call you back.

For general enquiries about PCI DSS, please call us on **0345 702 3344*****, selecting the option for 'all other enquiries'.

*If quarterly vulnerability scans are required as part of your compliance validation, then a passing scan result is required to complete your compliance status. If you or your service provider changes the way in which card payment data is collected, handled and/or processed, you must re-visit your PCI DSS validation requirements to ensure your compliance id still valid (Failure to update your PCI validation if changes are made will invalidate your compliance).

**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.

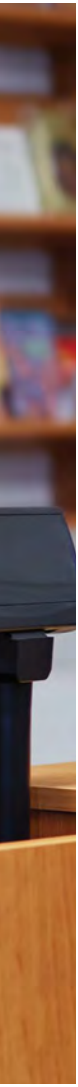
***We're open for card processing enquiries between 9am - 6pm Monday to Friday, excluding public holidays. To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide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

NEXT

## NEW OR REPLACEMENT MERCHANT ID'S FOR EXISTING CUSTOMERS AND PCI DSS

If you open an additional store, a new payment channel or there's a change in your legal entity and we issue you with a new Merchant ID (MID), you'll need to review your PCI DSS Compliance and take action. You'll have two months, from the date of your first transaction through your new MID, to achieve and validate your compliance with us. If you believe your existing compliance covers your new MID, you still need to let us know, otherwise your new facility will remain non-compliant and be subject to non-compliance charges.

PREV



# WHAT ARE MY NEXT STEPS

## GLOBAL FORTRESS/SECURITYMETRICS CUSTOMERS

If you're enrolled with Global Fortress/SecurityMetrics, please call them direct on **0330 808 1003*** to advise them of any changes that have taken place. This includes:

- Any replacement and/or additional MIDs.
- Any changes to the way you accept, handle, process, transmit and/or store your customer card data.
- Any new service provider or payment application used to handle and/or transmit your customer card data.

SecurityMetrics will review the scope of your new environment to check if your validation requirements have changed and if nothing has, they'll link your existing compliance to your new MID. If there have been changes, this might mean that you need to complete a new SAQ and/or quarterly vulnerability scans are now required. SecurityMetrics will guide you through this process and can help with any questions you may have.

## MERCHANTS REPORTING THEIR PCI DSS COMPLIANCE DIRECTLY TO US

Please review your existing compliance validation documentation to understand if this covers your new facility.

- If nothing has changed, please re-submit your documentation to us and confirm the compliance covers your new facility.
- If your compliance scope has changed, this means your existing compliance is no longer valid. Please review your new validation requirements and submit your new documentation to us as soon as possible.
- If you need help in understanding if your compliance validation requirements have changed, you will need to seek guidance from a QSA. Our QSA partner, SecurityMetrics, can be contacted on **0330 808 1003*** whereby they can offer a free consultation to confirm your validation requirements (for example whether you need to complete a SAQ and whether any vulnerability scans are needed).

**Please be aware that any new MID will be deemed non-compliant and liable for non-compliance charges until compliance has been validated to us.**

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 - 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.

***We're open for card processing enquiries 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

# CHANGES TO VISA'S ACCOUNT INFORMATION SECURITY (AIS) PROGRAMME

**Towards the end of 2015, Visa announced changes to their AIS Programme. This impacts businesses that aren't PCI DSS compliant, as well as revising the penalties for account data breaches.**

## WHY ARE THE CHANGES BEING INTRODUCED?

The changes are a response to the card processing community and their customers wanting to take a prioritised risk-based approach to their security and compliance activities. Consequently, the changes are designed to reflect and promote the need for increased awareness of, and responsibility for, making appropriately informed decisions on security and compliance. This was done with the understanding that where a failure occurs, the costs are appropriate to the risk.

## SUMMARY OF CHANGES

- Card processors are required to provide detailed explanations, by way of remediation plans, as to why their merchants are non-compliant as part of each reporting cycle.
- Card processors are to achieve and maintain 90% compliance across their merchant portfolios.
- The new Visa Account Data Compromise (ADC) event penalty regime became effective from **1st May 2016**.

## WHAT YOU NEED TO DO

In order to meet Card Scheme reporting requirements, you must continue to provide PCI DSS compliance updates (and scans if required for compliance purposes) to us on a quarterly basis.

Businesses who aren't PCI DSS compliant across any particular merchant level (PCI Level 1-4) will be required to provide their card processors with an explanation and a plan for the following 12 months, indicating how they'll ensure payment card data is protected.

PREV

## ADC EVENT PENALTY STRUCTURE

The revised penalties for new ADC events effective from **1st May 2016** are as follows:

- A per-event non-negotiable management fee of €3,000 to be charged for each ADC event;
- Penalties will be based on the number and value of cardholder data put at risk:
  - €18 for each PAN and CVV2
  - €3 for each PAN alone
- If the penalty exceeds €100,000, it'll be capped at 5% of the merchant's Visa Inc. gross annual purchase volume in the 12 months prior to the initial notification of the ADC event.
- Where 300,000 or more accounts indicate track data potentially at risk, the Global Compromised Account Recovery (GCAR) Programme may apply. As this is an existing global programme, no additional provision for magnetic stripe compromise will accrue in the Visa Inc. programme.
- Visa may apply penalty reductions based on a merchant's self-notification of a breach and their PCI DSS compliance status.

A business that experiences an ADC event, but who uses Verified by Visa (VbV), will receive a reduction in their penalty, up to a maximum of 50%, based on the number of VbV registered cards compromised. It should be noted that all penalties and reductions are at Visa's discretion and may vary depending on circumstances.

The card processing community is proactively communicating these changes to you in order to underpin the importance of achieving and maintaining PCI DSS compliance as an effective way of alleviating a potential ADC event.

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

*We're open for card processing enquiries 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

# 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 includes 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 not have taken the necessary precautions to safeguard your customer's data that you have outsourced to them.

## 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.

## 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.

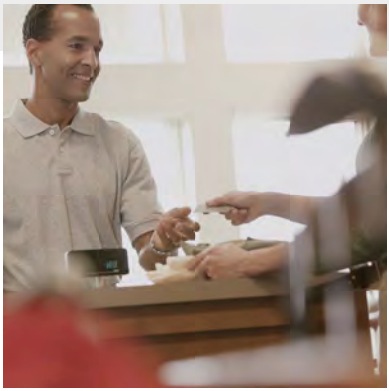
**"By self-reporting any suspected breach early, you can help to reduce the impact to your business and may reduce the possible penalties"**

NEXT

# RETAIL SPECIFIC NEWS

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/Realex Ecommerce Platform 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.



PREV

globalpayments

AUTUMN 2016

# RETAIL SPECIFIC NEWS

**INTERACTIVE EDITION** - KEEPING YOU IN THE KNOW

## IN THIS ISSUE



BEGIN

# CARD SCHEME UPDATES

## NEW MASTERCARD BIN RANGE

**Effective 14th October 2016**, MasterCard has announced that they're introducing a new series of Bank Identification Numbers (BINs) that begin with a "2". 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 new "2" series BINs will be processed the same way as MasterCard's existing BIN range that's between "51–55"**

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.

To ensure stores and online businesses are ready to accept cards featuring the "2" series BIN, MasterCard has confirmed that they'll launch a mystery shopper programme in early 2017. Companies who aren't able to accept the new cards could be liable to fines, so it's important you're prepared.

If you rent a terminal from us, you don't need to do anything as we'll automatically update it before the change comes into effect. If you own your own terminals or rent them from a third party, you'll need to contact your supplier to get them to upgrade your equipment so you can accept the new cards. If you've not yet done this, it's important that you do so now, so that you're ready if you're visited by one of MasterCard's mystery shoppers.

If you have any queries regarding this change, 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.

**"To ensure stores and online businesses are ready to accept cards featuring the "2" series BIN, MasterCard has confirmed that they'll launch a mystery shopper programme in early 2017"**

NEXT

# DEPLOYMENT OF CONTACTLESS CAPABLE TERMINALS

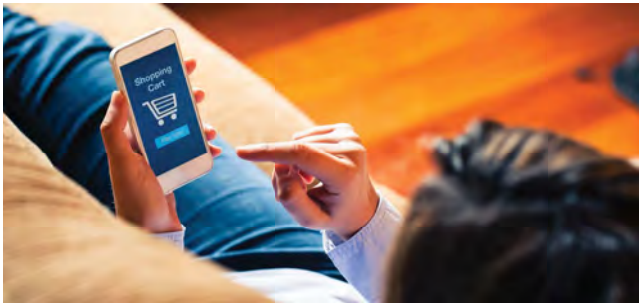
Visa has mandated that since **1st January 2016** any new terminal must be Contactless capable. This means if you're opening a new outlet or simply adding an additional terminal in an existing outlet, any new terminals that you place must support Contactless payments. Where an existing terminal is faulty 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 that 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 or adding an additional terminal in an existing outlet, any new terminals that you place must support Contactless payments."**




# MOBILE PAYMENTS AND THE FUNDING PAN

Mobile payment technologies, like Apple Pay, that allow cardholders to pay for goods using mobile phones or watches, make use of a disguised card number that's known as a tokenised PAN. With the rapid growth in this area, the Card Schemes (MasterCard and Visa) have mandated that the last four digits of the cardholder's actual card number (known as the funding PAN) must be returned to the terminal. This allows the cardholder to identify which card was used for a transaction, for example, when trying to work out which card they used for the original sale if a refund is needed.

To support this mandate we've updated our systems so that this information is included in the authorisation response message and can be printed on your transaction receipts. If you own your terminals or rent them from a third party, you'll need to contact your supplier to request they update your terminals so you include the funding PAN. However, if you rent a terminal from us, you won't need to do anything as we'll automatically update it over the coming months to add this information.

You can find more details on how to include the funding PAN in our 'Authorisation and Settlement Technical Specifications'. You'll find the latest version at our website **www.globalpaymentsinc.co.uk.** You'll need to log in to the Customer Centre using your merchant number and then select the option for 'Global Payments', followed by 'Documentation'. If you've got any queries regarding this change, 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

PREV

**"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"**

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**
- 1408 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.

NEXT

globalpayments

HOME PAGE

SERVICE. DRIVEN. COMMERCE

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



GP470