globalpayments

SPRING 2017

MERCHANT NEWS

INTERACTIVE EDITION - KEEPING YOU IN THE KNOW

IN THIS ISSUE

BEGIN

WELCOME TO THE SPRING 2017 EDITION OF MERCHANT NEWS

Nigel Hyslop
President and
Managing Director UK

In this first edition of Merchant News for 2017, you'll find features on Card Industry News, Product News and Card Scheme Updates. Please take the opportunity to read these as they contain important information that'll ensure you make the most of your card processing facility and keep you up to date on changes in the industry that may impact you. You'll also get the opportunity to download an eBook from our colleagues at Realex Payments. If you trade online, or you're thinking of moving into this sector, the eBook gives you more information about shopping carts and the different types available to you.

In the Autumn 2016 edition of Merchant News, I told you about the 'Global Peddlers' and their fund raising efforts for LOROS. I'm pleased to say that the peddlers were nominated for their efforts in the Best Corporate Social Responsibility Programme at this year's Card And Payment Awards ceremony held at Grosvenor House Hotel in London back in February. Disappointingly, they didn't win but they're riding again this year. This time they'll be raising funds for Rainbows, who are the East Midlands' only hospice for children and young people. I look forward to sharing more details on how the ride goes in a future edition.

All the best

Nigel Hyslop
President And Managing Director UK

"I'm pleased to say that the peddlers were nominated for their efforts in the Best Corporate Social Responsibility Programme at this year's Card And Payment Awards ceremony held at Grosvenor House Hotel in London back in February."

NEXT

WHICH SHOPPING CART IS BEST FOR YOUR CUSTOMER?

A NEW EBOOK ON THE BEST SHOPPING CART CHOICE HAS JUST LAUNCHED

We're pleased to unveil our brand new eBook - **'Select The Right Shopping Cart For Your Online Business'.** This is designed to help retailers choose the optimum ecommerce platform for their online store.

A shopping cart is essentially a piece of software that holds items while a customer shops, calculates the total cost, adds shipping and taxes and integrates with a payment gateway, like Realex Payments, which ultimately processes all the transactions. In recent years they've evolved to fulfil valuable new functions, helping ecommerce merchants to track, manage and fulfil orders. They also deliver valuable marketing support, with the ability to start loyalty programmes and even add a blog!

In our eBook we look at seven of the top performing global ecommerce software platforms across both 'OpenSource' and 'Software-as-a-Service' (SaaS) solutions. With the help of payments product experts, along with key customers, it provides valuable insight into the shopping cart selection process.

Here are the key criteria we used to evaluate each shopping cart:

- **Cost:** Setting a budget helps to set the tone for shopping cart selection so the eBook provides a cost estimate for some of the major shopping carts.
- **Ease Of Use:** Some customers just want a solution that has a user-friendly interface, while others will want lots of marketing and analytics features. We rate the carts by how easy they are to use on a day-to-day basis.
- **Customer Support:** If a business wants an expert at hand and available for support, a SaaS cart solution may suit best. We compare the different solutions to show the level of customer support applicable to each.
- **Customisation:** The level of customisation available is one of the key decision criteria on choosing a shopping cart so we break down each option by its ability to tailor to unique requirements.
- **Extras:** The eBook looks at the extras offered by shopping cart providers, like cross-selling functionality, recently viewed products and the ability to give coupons to shoppers.

You'll also find an in-depth feature about one of our inspiring customers, Emerald Green Baby, to give an insight into how they started selling online to China with the Magento shopping cart. You can download your free copy by visiting our website at: **https://www.realexpayments.com/ecommerce-guide-select-shopping-cart/.**

PREV

realex payments
A division of globalpayments

"We're pleased to unveil our brand new eBook - 'Select The Right Shopping Cart For Your Online Business."

NEXT

PRODUCT NEWS

HOMECURRENCYPAY UPDATE

Last summer we wrote to eligible customers who rent VeriFone terminals from us, to let you know we'd be upgrading your terminal with HomeCurrencyPay, our Dynamic Currency Conversion (DCC) service. 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.

We're delighted to advise that this upgrade has now been completed, which now means all the terminals types we rent to our customers, both Ingenico and VeriFone, can now offer this service. This allows even more of you the option to offer your international customers the ability to pay for purchases in their home currency or sterling. Using DCC also 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.

If you have any queries regarding HomeCurrencyPay, or if you rent a terminal from us and think this service 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.

"We're delighted to advise that this upgrade has now been completed, which now means all the terminals types we rent to our customers, both Ingenico and VeriFone, can now offer this service."

HomeCurrencyPay

BUSINESSVIEW

SELF SERVICE NOW AVAILABLE

Did you know that you can log into BusinessView – our integrated, web-based payment information management tool – and use the 'Self Service' option to make a change to a lot of the things you previously had to ring us for? This is also available on BusinessView Lite, our free of charge, 'lighter' version of BusinessView*.

By taking this route you can make changes to your:

- Contact and address details
- Your banking details

You can also:

- Raise requests to reprint reports and letters
- Report basic faults and incidents

This is great news and means you:

- No longer have to wait in a queue for your call to be answered.
- Don't have to rely on the postal service.
- can monitor the progress of your request online.

Some of the changes you can make are made instantly, you won't even need to wait for a response.

You'll find 'Self Service' by clicking on the option for 'Tickets'.

UNIONPAY

If you accept UnionPay cards, you can now view these transactions on BusinessView/ BusinessView Lite as well. You'll find them on all screens and reports as 'Card Type 37'.

SMART DISPUTE MANAGER (SDM)

BusinessView/BusinessView Lite also allows you to manage all your chargebacks online via SDM so you no longer have to use the post to send us secure documents. Just log in to BusinessView and you'll find SDM under 'Applications'.

DON'T HAVE ACCESS TO BUSINESSVIEW?

If all this sounds good but you don't currently use BusinessView or BusinessView Lite, just visit: **https://businessviewglobal.com/UK/** and click on the link to 'Register'. To find out more, please call us on 0345 702 3344**, selecting the option for 'all other enquiries'. Alternatively visit our website at: **https://www.globalpaymentsinc.com/en-gb/accept-payments/merchant-tools.**

*Charges apply for the full BusinessView service.

**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

CARD INDUSTRY AND CARD SCHEME NEWS

ENSURE YOU'RE CREDITED FOR YOUR TRANSACTIONS AND KEEP YOUR TERMINAL UP TO DATE

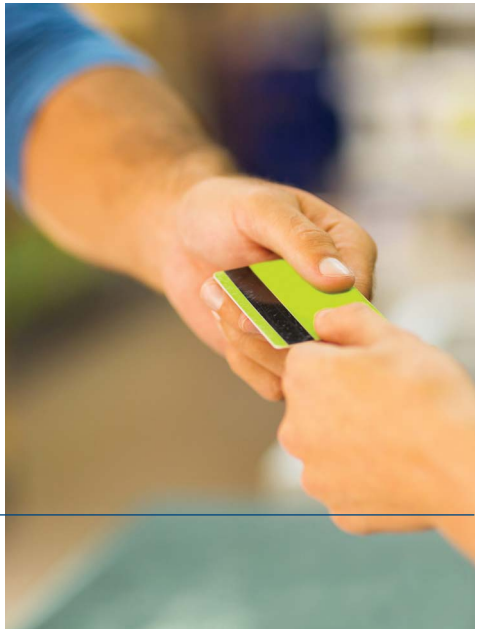
If you rent one of our terminals, it contacts us throughout the day to send us your transactions. However, we're unable to process these until you've completed an 'End Of Day' procedure on your terminal. You need to do this every business day, and by 2:00am at the latest. Not doing so will lead to delays in crediting your bank account and may also result in chargebacks. You can find specific details on how to do this in your terminal user guide.

By renting your terminal from us, we also ensure it's kept up to date with the latest software and complies with all the Card Scheme (Mastercard and Visa) regulations. To do this, your terminal must always be available for us to connect to so it must be:

- permanently connected to a power supply or its battery is fully charged, and
- connected to a telephone line that is able to make calls 24 hours per day, or for mobile terminals, that a GPRS signal is available.

If you have any queries regarding this, please contact us on 0345 702 3344*, selecting the option for 'Card Terminal, Global Iris or GLOBAL MPOS SUPPORT', followed by your terminal type.

*Lines are open every day (except Christmas Day) between 8.00am and 11.00pm Monday to Saturday, 10.00am and 5.00pm on Sunday and between 10.00am and 4.00pm on 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.



RECOVERED CARDS

REMOVAL OF FINANCIAL REWARD FOR RECOVERED VISA CARDS

Visa have announced that they'll no longer be providing a financial reward for any of their cards recovered at the point of sale as part of a 'Code 10' call.

It's still essential that you attempt to recover, and return, any cards that we ask you to retain as part of a 'Code 10' call, but you should not endanger yourself or your colleagues in attempting to do so.

You can find more details on Recovered Cards and Code 10 calls in your copy of our *Merchant Operating Instructions.* However, please remember that the reward detailed in there only now applies to recovered Mastercard cards.

RETIREMENT OF V1.X PIN ENTRY DEVICES (PEDS)

All PEDs that are used by cardholders to input their PIN number when making a card payment are certified to the Payment Card Industry PIN Transaction Security (PCI PTS). These are regularly revised to ensure that only the most up to date software is used, with devices using obsolete software being withdrawn. Following a review, devices certified as v1.x must be replaced by 31st December 2017.

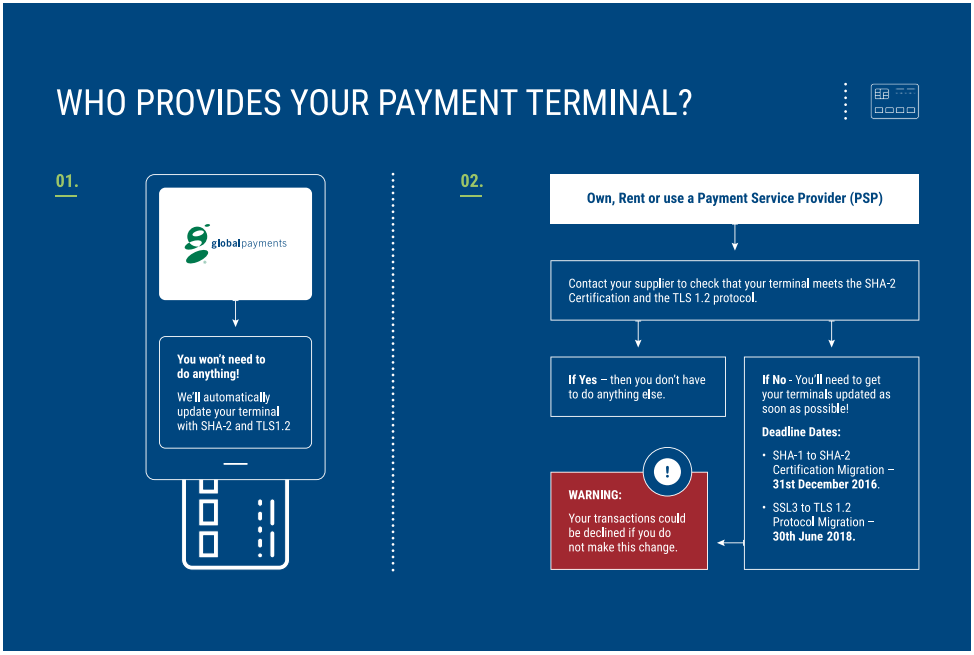
WHAT DO I NEED TO DO?

We've already started contacting our customers who rent a v1.x device from us that needs to be replaced. If we contact you, or have already contacted you to do this, please make every effort to assist us in arranging for your new one to be delivered and installed before the end of the year. That way you'll retain your PCI DSS compliance. If we've contacted you but you've not started this process yet, you can call us on 0345 702 3344*, selecting the option for 'all other enquiries' and quoting reference TRP PCI1 to arrange for your replacement to be sent.

*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

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



"If you accept card payments online or you have a terminal that connects to us via Internet Protocol (IP), these must be capable of supporting SHA-2 and TLS 1.2."

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 since 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) 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?

If you accept card payments online or you have a terminal that connects to us via Internet Protocol (IP), these **must** be capable of supporting SHA-2 and TLS 1.2

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, we've made the necessary upgrades to ensure that you already comply 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, and you've not already done so, you must 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 as your transactions could be declined if you don't.

If you have any questions regarding this important change, we've produced a series of frequently asked questions (FAQs), which you'll find at our website at: **www.resources.globalpaymentsinc.co.uk**. If these don't answer your questions, 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

REMINDER: MANDATORY REQUIREMENT FOR MASTERCARD AUTHORISATIONS

In 2014, 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 mandated a number of changes to how authorisations are processed. Although we told our customers about these requirements at the time, and we included the changes into your Card Processing Agreement, we want to remind you of the Mastercard rules so that you can avoid any unnecessary fees.

All Mastercard authorisations must be defined as either a 'Final Authorisation' or a 'Pre-Authorisation' and also flow the Schemes Reference Data (SRD). These changes apply to all transactions made on the following Mastercard brands: Mastercard Credit, Mastercard Debit, Maestro Debit and Maestro International.

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 seven calendar 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 seven calendar 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 and include the SRD in the clearing transaction.

MASTERCARD PRE-AUTHORISATIONS AND WHEN THEY SHOULD BE USED

Pre-Authorisations are used when the goods or services cannot be dispatched or delivered within seven calendar 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. Transactions flagged as a Pre-Authorisation will have a payment guarantee period of up to thirty 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.

PREV

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 seven calendar days of the original authorisation date.
- Where a payment guarantee period is required for up to thirty 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, a 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 us on 0345 702 3344* selecting the option for 'all other enquiries'. If you own your own terminals, rent them from a third party or use a Payment Service Provider (PSP) to accept payments online and are unsure whether your equipment can perform a Pre-Authorisation, you'll need to contact your supplier to confirm this.

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.

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 record must be created that contains the SRD, 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.

SCHEMES REFERENCE DATA

When you complete a Final Authorisation or Pre-Authorisation, a clearing record must be created that contains the SRD from the previous authorisation request. Failure to include this data will incur a Processing Integrity Fee (PIF) that can be easily avoided.

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

PAYMENTS CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) UPDATES

PCI DSS VERSION 3.2 (v3.2) AND THE IMPORTANCE OF PCI DSS COMPLIANCE

AN EVOLVING STANDARD

PCI DSS is a set of requirements designed to ensure the safe storage, processing and transmission of payment card data and applies to all businesses handling card data, which any business taking card payments needs to adhere to. It's regularly updated by the Payment Card Industry Security Standard Council (PCI SSC) to make sure the standard meets today's security needs.

v3.2 was released last year and all new PCI validations have had to meet the new standard since **1st November 2016**. For customers who 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.

WHAT'S NEW IN V3.2?

The release of v3.2 builds upon the release of previous versions by including clarifications and new requirements that are intended to ensure organisations are addressing emerging threats. In particular, to ensure that service providers are fulfilling their responsibilities in providing services to other organisations. Please take the time to visit the PCI SSC website for the full details of the new standard at: **https://www.pcisecuritystandards.org/index.php**.

If you have any queries regarding your requirement to be PCI DSS compliant, please call us on 0345 702 3344** selecting the option for 'all other enquiries', or alternatively, you can email us at **customer.services@globalpay.com**.

THE IMPORTANCE OF COMPLIANCE

If you're not PCI DSS compliant, in accordance with your Card Processing Agreement, we may apply a monthly non-compliance charge until you reach compliance. To help you achieve and maintain compliance, we've developed Global Fortress in partnership with SecurityMetrics, a Qualified Security Assessor (QSA). This service gives you access to the resources you need to help you safeguard your customer data and avoid our monthly non-compliance charge.

"v3.2 was released last year and all new PCI validations have had to meet the new standard since 1st November 2016."

NEXT

Global Fortress

PREV

THE KEY BENEFITS OF GLOBAL FORTRESS INCLUDE:

- Access to Security Metrics, our QSA partner, who'll support you in taking the necessary steps to achieving compliance.
- Simple one stop shop to compliance for a small monthly fee.
- You'll be billed through us so there's no requirement to hold contracts with multiple companies.

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 the above number selecting the option for 'stationery' and we'll 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 'Card Processing'. You can also find out more about PCI DSS by visiting the Global Fortress website at **www.globalfortress.co.uk** or call SecurityMetrics directly on 0330 808 1003***.

WHAT'S THE ALTERNATIVE TO GLOBAL FORTRESS?

You are free to use the services of another QSA, or complete a Self-Assessment Questionnaire (SAQ). If you wish to do this, please inform us and provide proof of your compliance to avoid the monthly non-compliance charge.

"You are free to use the services of another QSA, or complete a Self-Assessment Questionnaire (SAQ)."

YOU CAN DO THIS IN EITHER OF THE FOLLOWING WAYS:

- Email your documents (quoting the last 4 digits of your Merchant ID e.g. XXXX4321) to **saq@securitymetrics.com.**
- Post your documents (quoting your Merchant ID) to PCI DSS Compliance Programme, Global Payments, 51 De Montfort Street, Leicester, LE1 7BB.

This alternative will incur an administrative fee, which starts from £3.00 per merchant ID per month (plus VAT, where applicable). If you enrol with Global Fortress and complete the required steps, your compliance will be automatically reported to us by SecurityMetrics. You won't need to send proof of your compliance directly to us.

*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 is still valid. Failure to update your PCI validation if changes are made will invalidate your compliance.

**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.

***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 0330 numbers.

NEXT

A GUIDE TO SAFER PAYMENTS

We know protecting your customers' card data can be a daunting prospect but the penalties for losing it can be severe. Fines from the Card Schemes (Mastercard and Visa), as well as the corrective work needed following a data breach, can sometimes run into tens of thousands of pounds for your business. The Payment Card Industry Security Standard Council (PCI SSC) have issued guides that can help you with this.

HOW CAN THESE GUIDES HELP ME?

Below you'll find more details of the guides, which provide you with plenty of hints and tips to help you maximise your data security.

- **Guide to Safe Payments:** This provides you with some simple methods to increase the security of your business, inclusive of the apparent cost, ease of implementation and the amount of risk reduction that you could benefit from.
- **Common Payment Systems:** This outlines the most common payment systems that are in use, the risk and threats that they could be susceptible to, and recommendations to help protect your business.

You'll find both these guides, together with others than can help your business manage the safe handling of cardholder data, by visiting **https://www.pcisecuritystandards.org/document_library**. In the 'Search' area you'll need to filter by 'Guidance Documents' then 'Small Merchants'.

Remember, your customers' data is vulnerable. By following the guidelines and principals provided by the PCI SSC you can better safeguard against a data breach and avoid a heavy penalty.

PREV

"The PCI SSC have issued guides that can help you protect your customers' card data."

NEXT

ARE YOUR MERCHANT AGENTS PROTECTING YOUR DATA?

The world of online payments is becoming more sophisticated so you may be using a number of Merchant Agents, also known as Service Providers, for your business.

WHAT ARE MERCHANT AGENTS?

Web hosting companies, payment gateways and shopping cart providers are all examples of Merchant Agents. These may directly or indirectly be involved in storage, transmission or processing of cardholder data on your behalf. Do you know who all your Merchant Agents are and more importantly are they Payments Card Industry Data Security Standard (PCI DSS) compliant?

WHAT ARE THE RISKS TO MY BUSINESS?

Merchant Agents can be targeted by criminals because of the large volume of card data they hold on behalf of the many businesses that they service. If your third party fails to protect this data and were to suffer a breach, they could jeopardise your business. Ultimately, you're responsible for the data that your agent or provider processes for you and you could be liable for any penalties that the Card Schemes (Mastercard and Visa) may apply, which can easily reach tens of thousands of pounds.

WHAT DO I NEED TO DO?

As well as the requirement for your Merchant Agents to be PCI DSS compliant, Visa Europe mandates that they must also be registered with Visa directly before they can become a service provider for any business. By registering with Visa an agent demonstrates that they're PCI DSS compliant at the time of registration, they're able to meet a minimum set of security standards and show that they follow acceptable business practices to protect the data they handle.

HOW DOES A MERCHANT AGENT REGISTER WITH VISA?

Visa's website **https://www.visaeurope.com/receiving-payments/security/downloads-and-resources** provides guidelines for both you and your Merchant Agents to follow to ensure that your agents become PCI DSS complaint, if they're not already.

"By registering with Visa an agent demonstrates that they're able to meet a minimum set of security standards and show that they follow acceptable business practices to protect the data they handle."

NEXT

DO YOU KNOW ABOUT SENSITIVE AUTHENTICATION DATA (SAD)?

WHAT IS SAD?

SAD is used to assist the authorisation process of transactions to check that the genuine cardholder has authorised it and include:

- **Card Security Code (CSC) Or 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), or on the front of American Express cards, used for authenticating Cardholder Not Present (CNP) transactions.

- **The PIN Code**

  This is used by the cardholder to authenticate a face to face transaction, either at an ATM or at a payment machine such as a terminal in a shop.

- **Track Data**

  The data contained within the magnetic stripe on the back of a payment card, used during swipe transactions either at an ATM or at a payment machine such as a terminal in a shop.

WHY IS STORING SAD PROHIBITED?

SAD is used by the card issuer to verify and approve transactions. It's vital that this data is protected to ensure only the genuine cardholder can use it to authorise a transaction. Storing SAD after an authorisation has been made is a violation of both the Payment Card Industry Data Security Standard (PCI DSS) and Card Scheme (Mastercard and Visa) Rules and it should be securely erased or shredded.

Visa has reinforced the importance of not storing SAD in its Account Data Compromise penalty structure. If you're breached and only the card number is compromised a fee of 3 per item is be applied, however, this increases to 18 if CVV has also been compromised. You can find more details about this in the next article.

"SAD is used by the card issuer to verify and approve transactions. It's vital that this data is protected to ensure only the genuine cardholder can use it to authorise a transaction."

GUIDANCE ON PCI DSS

For further guidance on how to protect SAD and comply with the PCI DSS, please contact a Qualified Security Assessor (QSA) and/or take the time to visit the PCI Security Standards Council website: **www.pcisecuritystandards.org/index.php**. This provides lots of information and supporting documentation regarding the requirements of SAD storage and general advice to help you achieve and maintain your PCI DSS compliance. 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 0845 602 4818.

NEXT

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

In the Autumn 2016 edition of Merchant News, we told you about Visa's changes to their AIS Programme. Here's a reminder of these changes and the impacts to businesses that aren't Payment Card Industry Data Security Standard (PCI DSS) compliant, and the possible penalties for account data breaches.

WHY WERE THE CHANGES INTRODUCED?

The changes were 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 were 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.

AIS ACCOUNT DATA COMPROMISE (ADC) PENALTY STRUCTURE

Penalties for new ADC events 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.
- A merchant that experiences an ADC event but uses Verified by Visa (VbV) will get up to a maximum of 50% reduction in the penalty, based upon the number of cards compliant with VbV.

Visa may apply penalty reductions based on a merchant's self-notification of a breach and their PCI DSS compliance status but these reductions are at their discretion. If you store Sensitive Authentication Data (SAD), the higher per item fee of 18 will be charge for each individual card number put at risk.

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.

PREV

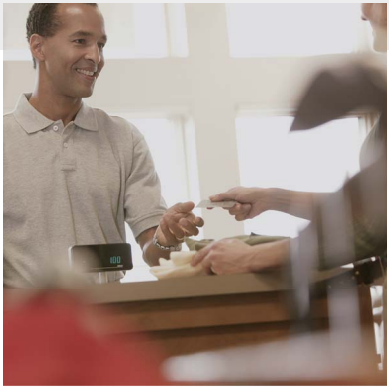
"Visa may apply penalty reductions based on a merchant's self-notification of a breach and their PCI DSS compliance status but these reductions are at their discretion."

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.

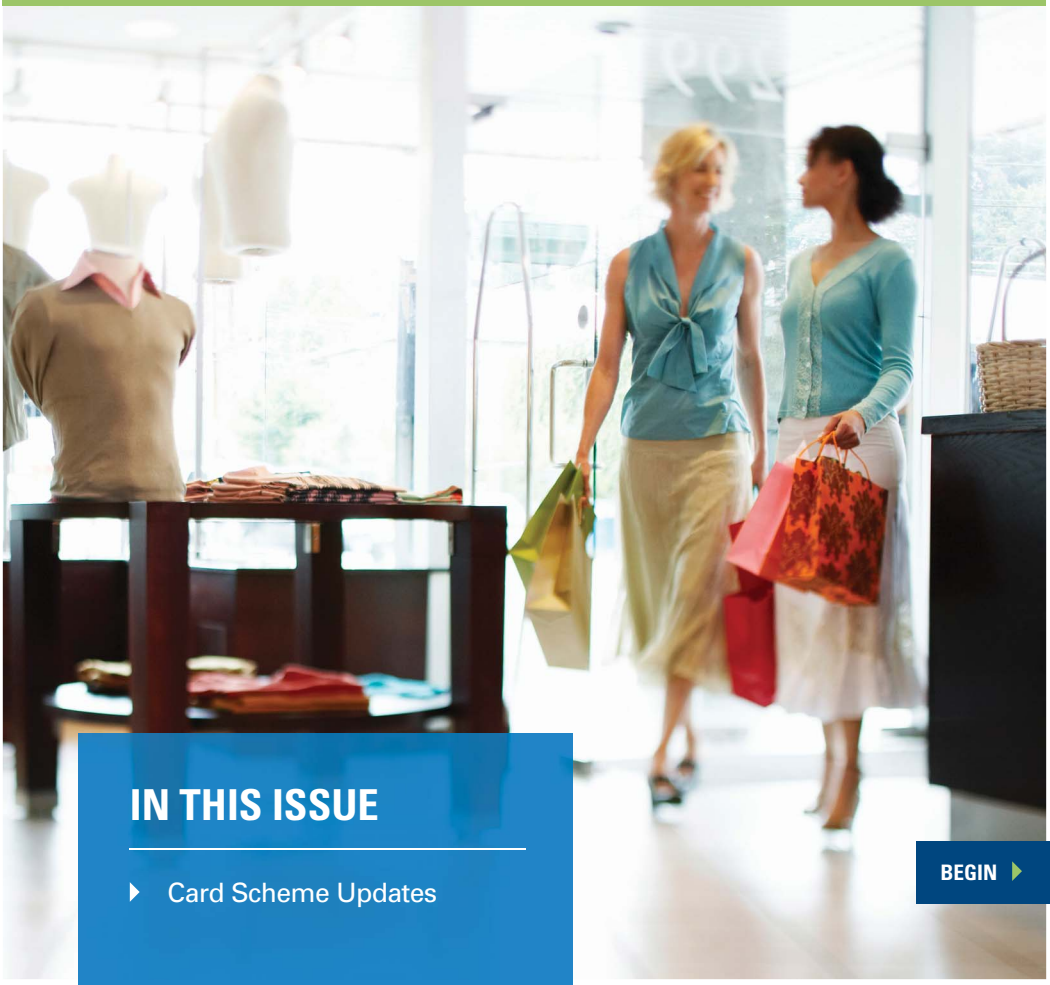


globalpayments

SPRING 2017

RETAIL SPECIFIC NEWS

INTERACTIVE EDITION - KEEPING YOU IN THE KNOW



IN THIS ISSUE

BEGIN

ECOMMERCE TRANSACTIONS NEED TO BE CORRECTLY FLAGGED

Do you trade online and use a Payment Service Provider (PSP) to process transactions? If you do, you must ensure that you include the correct Universal Cardholder Identification Field/Cardholder Authentication Verification Value (UCAF/CAVV) data in the authorisation and settlement messages for secure ecommerce transactions.

The Card Schemes (Mastercard and Visa) have reiterated the importance of including the UCAF/CAVV data in ecommerce transactions. Failure to correctly flag them with the output from the 3D Secure process can result in loss of liability shift, delays to your transactions being processed, and possibly their rejection.

Full details of the relevant fields can be found in our 'Authorisation And Settlement Technical Specifications' guide, which you can find on our website: **www.globalpaymentsinc.co.uk**. You'll need to log in to the Customer Centre, using your Merchant Number and select the option for 'Documentation'.

Although your ecommerce solution is provided by a PSP, it's your responsibility to ensure your transactions are submitted correctly. Therefore, please contact your service provider to ensure that the message contents of your ecommerce transactions are correct.

"Failure to correctly flag ecommerce transactions with the output from the 3D Secure process can result in loss of liability shift, delays to your transactions being processed, and possibly their rejection."

CORRECT FLAGGING OF AUTHORISATION STATUS IN AUTHORISATION REQUEST MESSAGES

When you authorise a transaction, it needs to be flagged as either an Estimated Value Authorisation or an Actual Value Authorisation. Estimated Value Authorisations are used when the final amount of the transaction is not known, for example, when checking into a hotel. An estimate of the guest's final bill can be made but this may be subject to change during the course of the stay. Actual Value Authorisations are used when the final amount of the transaction is known, for example, the purchase of an item in a retail outlet. This is done by populating the authorisation status flag in the authorisation request message with either an 'E' for an Estimated and 'A' for an Actual (or Final) Value Authorisation.

Earlier in Merchant News you'll have read about the steps you need to follow so you meet Mastercard's requirements around the authorisation of transactions. Visa have now advised that they'll also be differentiating between Estimated Value Authorisation and Actual Value Authorisations. They require that the authorisation status field is correctly populated.

It's essential that the authorisation status field in the authorisation request message is correctly populated to ensure that authorisation requests are processed correctly. If you rent your terminal from us, you don't need to take any further action as we'll update it to ensure that you meet these requirements.

If you don't rent your terminal from us, you must contact your terminal supplier to ensure that your terminals are flagging the correct authorisation status values in the authorisation request message. Full details of the relevant fields can be found in our 'Authorisation And Settlement Technical Specifications' guide, which you can find on our website: **www.globalpaymentsinc.co.uk**. You'll need to log in to the Customer Centre, using your Merchant Number and select the option for 'Documentation'.

Not updating your terminals could lead to transactions being processed incorrectly and might also result in non-compliance fines being applied at a later date.

NEXT

IS YOUR TERMINAL CERTIFIED TO THE LATEST CARD INDUSTRY SPECIFICATIONS?

The Card Schemes (including Mastercard, Visa and American Express) have asked us to remind our customers of the importance of ensuring that all aspects of their terminal software is kept up to date with the latest Card Scheme, Payment Card Industry Security Standard Council and EMVCo specifications. Failure to do so may result in your terminal not processing certain card types correctly and could lead to Card Scheme fines.

If you rent your terminals from us, you don't need to take any further action as we ensure they're kept up to date with the latest software and comply with all the regulations.

If you own your own terminals or rent them from a third party, you'll need to contact your supplier to ensure that your terminals contain the most up to date software, which complies with all the latest card industry regulations.

"If you own your own terminals or rent them from a third party, you'll need to contact your supplier to ensure that your terminals contain the most up to date software, which complies with all the latest card industry regulations."

NEXT

REMINDER: RETIREMENT OF V1.X PIN ENTRY DEVICES (PEDS)

Please remember that by 31st December 2017, all PEDs certified to Payment Card Industry PIN Transaction Security (PCI PTS) v1.x must be replaced with a newer device that's approved to either v2.x or v3.x. If you don't replace any v1.x PEDs you'll be deemed as being non-compliant with the Payment Card Industry Data Security Standard (PCI DSS) at the start of 2018 and you may be charged a non-compliance fee.

WHAT DO I NEED TO DO?

If you rent your PED from a third party, you'll need to contact your supplier to confirm if this needs to be replaced or not. If you have a non-compliant device and it isn't replaced by the end of 2017, you'll no longer be PCI DSS compliant and may incur non-compliance charges.

REMINDER: SCHEMES REFERENCE DATA

To help improve the accuracy of a cardholders available funds, aid in the detection of card fraud and allow the linking of authorisations to the subsequent transactions, Mastercard and Visa require a unique reference number to be included throughout the lifecycle of all card transactions. Visa refers to this data as the Transactions Identification Number (Trans ID) whereas Mastercard refers to it as the Trace Identification Number (Trace ID). Generically they are referred to as the Schemes Reference Data or SRD.

If you own your own terminals, rent them from a third party or use a Payment Service Provider (PSP) to accept payments online, you're responsible for ensuring that all transactions contain the SRD. Failure to include this could result in data integrity charges or fines being levied by Mastercard and Visa which you'll be liable for.

"Visa and Mastercard require a unique reference number to be included throughout the lifecycle of all card transactions."

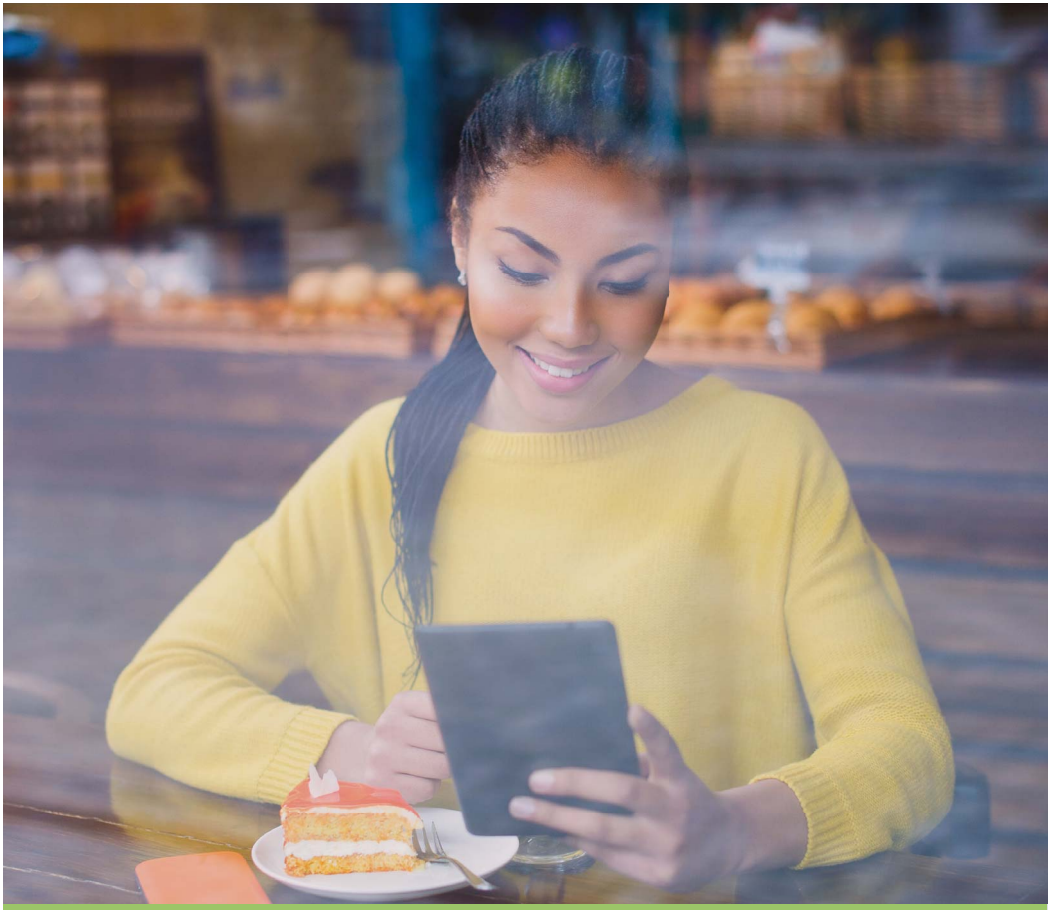
If you have any questions about these mandatory changes, please call on 0345 702 3344* selecting the option for 'all other enquiries'.

*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

globalpayments

HOME PAGE



SERVICE. DRIVEN. COMMERCE

Global Payments is HSBC'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.

GP528