globalpayments

Know the Risks

Things You Should Know Before You Start to Accept a Card Transaction

SERVICE. DRIVEN. COMMERCE

globalpayments

Contents

We want your business to accept cards without problems, however, it's vital you're aware of, and understand, the risks associated with accepting cards. This document is only a summary of these risks and you must also read and understand the *Merchant Operating Instructions* and the *Terms of Service*.

Chargebacks

One such risk is a chargeback, which is an unpaid card transaction that has been returned to us by the card issuer. We may debit the chargeback to your account, however, this document highlights some of the ways you can minimise the risk of chargebacks to your business.

There's no guarantee of payment for any transaction, even if you obtained authorisation. Authorisation checks that at the time of the transaction, the card isn't reported lost or stolen and that the genuine cardholder has sufficient funds available. Authorisation cannot verify that the genuine cardholder is conducting the transaction.

Note: Never spread the value of a transaction over more than one card, or split it into smaller amounts to achieve a successful authorisation. This is prohibited. This is not to be confused with splitting the sale between multiple cardholders, for example, when paying for a meal. This isn't prohibited.

Card Present (CP) Transactions

CP is where the card or Contactless payment device and the cardholder are physically present at the time of the transaction.

CP transactions can be accepted and verified in a variety of ways, including:

- Chip and PIN
- Chip and signature
- Contactless
- Magnetic stripe and PIN
- Magnetic stripe and signature

The best way to minimise the risk of CP chargebacks is to carefully follow the prompts provided by your terminal. If the terminal authorises a payment and prompts the cardholder to sign, then this should be allowed, subject to the normal checks associated with a signature-verified transaction (refer to 'Checking Cards' in the *Merchant Operating Instructions*).

Your terminal will automatically seek authorisation of the transaction depending on the floor limit set in the card by the card issuer and method of acceptance, for example, magnetic stripe verified by signature. However, if you are using Fallback paper vouchers due to a terminal fault, power failure etc., you must obtain a telephone authorisation for each transaction. Refer to 'Authorisation' in the *Merchant Operating Instructions*.

Note: Paper vouchers cannot be used as Fallback if a Mobile POS Solution fails. You must ask the cardholder for an alternative means of payment.

Chip and PIN Transactions: Chip and PIN cards and terminals have made substantial advances in preventing card fraud and are now the norm. All CP transactions must be completed using a chip and PIN terminal when presented with a chip and PIN card.

When your electronic terminal is unable to read the chip, it will prompt you to revert to the magnetic stripe on the card.

Contactless Transactions: Where your terminal is enabled to accept Contactless payments, the Contactless symbol will be displayed for low value transactions. The cardholder simply taps their card or Contactless payment enabled device to the reader to make the payment.

From time to time your terminal may request that a PIN transaction is completed instead of a Contactless one, when a card is used. This is an added security feature, designed to confirm that the cardholder is in possession of their card and you must continue with a chip and PIN transaction in the usual way.

Where your terminal is also enabled to accept Contactless High Value Payments (HVP), the Contactless symbol will be displayed for all transactions. HVP requires a Contactless payment enable device, for example, a smart phone.

If a card isn't enabled for Contactless, the customer doesn't have a Contactless enabled payment device, or they simply prefer to use the chip and PIN functionality, then the Contactless option can be bypassed by them inserting their card into the card reader to complete the transaction via chip and PIN.

For more information on Contactless, refer to 'Contactless Card Payments' in the *Merchant Operating Instructions*).

Magnetic Stripe Transactions: There are still many legitimate cards in circulation that contain no chip and you'll have to swipe the magnetic stripe. You may then have to use the cardholder's signature to verify the transaction, subject to the normal checks (refer to 'Checking Cards' in the *Merchant Operating Instructions*).

If your terminal is unable to read the chip on a card, it'll prompt you to swipe the card and continue the sale as a magnetic stripe transaction. This process is known as 'fallback to magnetic stripe'. Pay particular attention to these transactions as the chip could have deliberately been interfered with to avoid validation via the PIN. Check if there has been any visible attempt to remove, replace or damage it.

Note: Mastercard will decline transactions that fallback to magnetic stripe. It's important that your staff understand that if they can't accept a transaction using the chip on a Mastercard card, it'll be declined if they fallback to magnetic stripe. If the chip fails, please ask your customer to pay by an alternative card or method.

Key-entered Transactions: When the cardholder is present and the electronic terminal cannot read the card via the chip or magnetic stripe, then you may key-enter the details into your terminal. You must still seek online authorisation.

Note: This option isn't permitted for Maestro or UnionPay transactions and you should ask the cardholder for an alternative method of payment.

Note: If a card is accepted using this method and the transaction turns out to be fraudulent; you'll be liable for a chargeback and financial loss to your business. In this scenario, you may wish to ask for an alternative method of payment.

Card Not Present (CNP) Transactions

CNP is where you, the card and the cardholder are **not** all present together, for example, a transaction made over the internet, by mail order or telephone order (MOTO), or a recurring transaction. These situations are ideal for fraudsters because the card, signature and the personal identification number (PIN) cannot be checked. The majority of chargebacks result from transactions being undertaken fraudulently. If you proceed with a transaction that you are unsure of, you are doing so at your own risk. If the transaction has been completed, but the goods not despatched, you are still in a position to carry out a refund.

To minimise your risks:

- Be cautious of customers who give mobile phone numbers as their only form of contact.
- Be wary of an order emanating from an email account where the customer's name isn't reflected in the email account address.
- Be suspicious with transactions that have an unusually high value or volume for your type of business or the sale is 'too easy'. In our experience these are the more likely ones to be fraudulent.
- When performing a refund, always refund to the same card used for the original transaction.
- Keep a database of chargeback history to help identify patterns of fraudulent transactions. If a sale seems too good to be true then it probably is. Don't be afraid to contact the cardholder to ask further questions or request additional identification. A genuine customer should be pleased you're security minded and trying to protect them from fraud.
- Where possible, perform Address Verification Service (AVS) and Card Security Code (CSC) checks. Refer to your terminal manual or terminal supplier for assistance on using this security feature. Remember, you are **not** allowed to store the CSC data.
- For ecommerce transactions, an additional layer of security can be incorporated into websites. Mastercard SecureCode and Verified by Visa (VbV) have been developed to allow customers to authenticate themselves as the genuine cardholder. **To accept Maestro cards over the internet, you must support Mastercard SecureCode.**
- Always send goods by recorded or special delivery or by a reputable security carrier. Insist on a signed (preferably by the cardholder) and dated delivery note. Tell the courier not to make the delivery if the premises appear to be vacant. Please note that proof of delivery alone isn't sufficient evidence to defend a chargeback.
- Don't release goods to third parties such as taxi drivers and messengers.
- Be cautious of transactions where the billing address is different to the requested delivery address. Avoid delivering to addresses other than the cardholder's, such as hotels, internet cafes and 'care of' addresses.
- Be wary of requests for next-day delivery, requests to alter the delivery address at short notice, or telephone calls on the day of delivery requesting a specific delivery time.
- If a customer requests to collect the goods, perform the transaction at the time of collection through your point of sale equipment.

Note: You risk receiving a chargeback if the transaction is successfully disputed. We may debit the value of the transaction to your business. If you're at all suspicious, make a 'Code 10' authorisation call.

Remember… authorisation is NOT a guarantee of payment.

Copies of Sales Vouchers

We may request copies of sales vouchers at any time. Please respond immediately to any such request as failure to do so may result in a chargeback. Always retain a copy securely for your own

records. Please note that you should retain all transaction vouchers for five years following the delivery of goods or completion of the service provided.

Processing Third Party Transactions

Processing transactions on behalf of another business can severely damage your financial wellbeing. If you're either offered a lump sum for allowing unlimited access and usage of your card processing facility or a commission for each payment you process, be wary that it's very rare for the third party to deliver the service that was promised. Often these entities, whilst appearing to be genuine and providing plausible reasons for requiring assistance, are fronts for organised criminal gangs engaged in timeshare or ticketing scams.

You must **never** accept transactions on this basis. These transactions are usually disputed or fraudulent and could result in chargebacks and financial losses to your business. Should this be the case you'll be fully liable for reimbursing the cardholders where non-provision of the goods or services has occurred.

Third party processing also breaches your Card Processing Agreement with us, and identification of such activity may result in immediate suspension and eventual termination of your card processing facility. This type of processing can also lead to criminal proceedings.

If a third party approaches you, or your staff, to process their transactions, say no and contact us straight away with as much detail as possible. If you feel your business may have already succumbed to such a deception, or has recently received an approach, then please call us immediately for assistance with as much information as possible so that we can take appropriate action.

Terminals

Whether you rent a terminal from Global Payments or not, you're responsible for the terminal equipment and we strongly recommend that due consideration is given to the positioning and control of such equipment. You'll be responsible for any losses resulting from interference by third parties not authorised to manipulate the equipment in any way other than in the normal course of the transaction, for example, entering a PIN. Therefore, please consider the length of time you give to the cardholder to input their PIN details.

Note: Ensure that any surveillance equipment you have isn't able to record a cardholder entering their PIN.

Data Security

Security of personal data is a growing concern. Criminals are always looking at ways of getting this type of information from different sources. A vulnerable point of compromise which fraudsters have identified is card financial data which has been collected during the acceptance of cards. The Payment Card Industry Data Security Standard (PCI DSS) is a global mandated standard which has been supported by the Card Schemes to bring a greater level of security to this type of data.

As you're accepting card transactions, you need to be aware of the value of the data you collect when undertaking a card transaction and the need to secure it. If you were to suffer a security breach, there's a significant risk of financial and reputational loss to your business.

Note: Under your Card Processing Agreement with us, you're required to achieve and maintain PCI DSS compliance.

What's PCI DSS?

PCI DSS is a set of 12 comprehensive requirements for enhancing customer card data security, including requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Its purpose is to help organisations proactively protect their customer card data. Essentially, this is the personal, sensitive data stored on or in the card that is key to making a transaction. If you don't properly protect this data, fraudsters may find your system's vulnerabilities and hack in to steal it. The data is very valuable to them as they can use it to fund further illegal activity.

This is a very real risk. Every year merchants of all sizes suffer data breaches. These can result in fines from the Card Schemes because customer card data was not secured effectively and to the PCI DSS standards. These penalties start at €5,000 but dependant on the specific circumstances can be much more. In addition there will also be remedial costs to your business.

For further details on PCI DSS you can visit:

- http://www.pcisecuritystandards.org – this site holds the latest version of the PCI DSS specifications and guidance on how to become compliant
- http://www.mastercard.com/us/sdp/merchants/index.html
- http://www.visaeurope.com/receiving-payments/security.

What You Need to Do

Under your Card Processing Agreement with us, you're required to achieve and maintain PCI DSS compliance. We require **proof of your compliance with PCI DSS within two months of processing your first transaction.**

All merchants will fall into one of four merchant levels based on transaction volume over a 12-month period. The following guide indicates the volume of transactions at each level and the validation method you must employ.

Level	Criteria	Validation Action	Validation By
1	Over 6,000,000 Mastercard or Visa transactions a year	• Annual on-site security audit (including a Report on Compliance (ROC) • Quarterly network scans	Qualified Security Assessor (QSA)
2	Between 1,000,000 and 6,000,000 Mastercard or Visa transactions a year	• Annual on-site security audit (including a ROC) • Quarterly network scans	QSA or Internal Security Assessor (ISA)
3	Between 20,000 and 1,000,000 ecommerce transactions per year	• Annual PCI Self-Assessment Questionnaire (SAQ) • Quarterly network scans	QSA or Self Assessment
4	Below 20,000 ecommerce transactions and below 1,000,000 transactions per year	• Annual PCI SAQ • Quarterly network scans	QSA or Self Assessment

A full list of accredited QSAs can be found on the PCI Security Standards Council website:

https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

The following website provides details on how to become an ISA:

https://www.pcisecuritystandards.org/approved_companies_providers/internal_security_assessors.php

Introducing Global Fortress – Level 3 and 4 Merchants

To help you achieve and maintain PCI DSS compliance, we have developed **Global Fortress.** The key benefits of **Global Fortress** include:

- this service gives you access to the resources and guidance you need to help you safeguard your customer data
- a simple one stop shop to compliance that costs **from as little as £3.50[1] a month** per merchant ID (plus VAT, where applicable), invoiced monthly in arrears. When you sign up for **Global Fortress** the remainder of the current month will be free
- access to SecurityMetrics[2], our Qualified Security Assessor (QSA) partner for this product, who'll support you in taking the necessary steps to achieving compliance.

It's important that you act now to start your compliance journey so please call SecurityMetrics on 0330 808 1003* or visit www.globalfortress.co.uk to sign up.

What's the Alternative to Global Fortress?

You may prefer to achieve compliance through an alternative QSA or complete a Self Assessment Questionnaire (SAQ). SecurityMetrics will be able to provide you with the appropriate SAQ, so call them on 0330 808 0831*. Alternatively, you can download them from the PCI Security Standards Council website at www.pcisecuritystandards.org.

Should you wish to do this, please inform us and provide proof of your compliance. This alternative will incur an administrative fee which starts from £3.00 (plus VAT, where applicable)[3] per merchant ID, per month charged by us to cover the cost of additional work we will have to perform on your behalf. This will be in addition to any fees charged to you by your alternative QSA.

It's our responsibility to verify your compliance status and register you with Mastercard and Visa. Therefore, please ensure you provide us with a copy of: your certificate of compliance (annually), and your scan results (quarterly) if applicable. If you use a third party (other than Global Payments E-Commerce Platform) and/or a Payment Service Provider (PSP), a copy of their certificate of compliance is also required.

Please send copies of your completed documentation to us at:

PCI DSS Compliance Programme
Global Payments
51 De Montfort Street
LEICESTER
LE1 7BB

Or email them to saq@securitymetrics.com.

If you enrol for **Global Fortress,** your compliance with PCI DSS will automatically be reported to us, so you won't have to provide us with your completed documentation.

Level 1 and 2 Merchants

You will need to provide us with evidence of your ongoing PCI DSS compliance. Therefore, please send us the following:

- your Attestation of Compliance (AOC)/ROC (annually) for level 1 or 2 merchants
- your network scans (quarterly), if required
- if you use a third party (other than Global Payments E-Commerce Platform), a copy of their AOC.

Please send these to your Relationship Manager (RM) or the address above. Please speak to your RM or call our helpdesk on 0345 702 3344**, selecting the option for 'all other enquiries', if you need any further information.

Third Party Companies

If you're using a third party company and give them access to card and financial data for any purpose (for example, processing transactions, storing data or call centre functions), you'll need to ensure that they also adhere to all rules and regulations governing card data security. In particular, all third parties storing or processing this data on your behalf are required to be PCI DSS compliant. Any violations of these requirements by your third party are your responsibility and may result in you having unnecessary financial exposure.

A copy of their AOC is required. Please send it to the address detailed above.

What Happens If I Don't Become Compliant?

Level 3 and 4 Merchants

If you don't validate your compliance, we will apply a **monthly non-compliance charge of £0.15 for each sale transaction we process on your behalf, subject to a minimum monthly charge of £75.00** per merchant ID, for each month you remain non-compliant. The charge will be applied the following month in arrears and is not refundable.

You can easily avoid this monthly non-compliance charge by achieving and maintaining PCI DSS compliance.

Whichever route to compliance you choose, you will not be considered compliant with the PCI DSS requirements until we have received and registered your compliance status with the Card Schemes. Unless we receive valid proof of your compliance, this could mean we will apply the monthly non-compliance charge of £0.15 for each sale transaction we process on your behalf, subject to a minimum monthly charge of £75.00, as well as any monthly Global Fortress or administration fees.

Sign up now for **Global Fortress** to avoid this monthly non-compliance charge, and possible fines by the Card Schemes, and keep valuable customer card data secure by achieving and maintaining PCI DSS compliance.

Please call SecurityMetrics on 0330 808 1003* to sign up or provide proof of your PCI DSS compliance. You can also visit www.globalfortress.co.uk.

SecurityMetrics may call you to discuss Global Fortress, but if you do not want this to happen, then you must call us, within 14 days of receiving your merchant ID, on 0345 702 3344, selecting the option for 'all other enquiries', and advise us what alternative arrangements you will make to achieve compliance.**

Level 1 and 2 Merchants

Level 1 and 2 merchants are subject to different non-compliance charges and you will be sent written notification if these are applicable.

[1]**Price -** Global Fortress fees start from £3.50 per merchant ID per month (plus VAT, where applicable) where no vulnerability scans are required. If vulnerability scans are required, the fee is £7.00 per merchant ID per month (plus VAT, where applicable), allowing unlimited scanning of up to 3 URLs per merchant ID. If additional scans are required, you will need to pay an additional fee direct to SecurityMetrics.

Prices for merchants with 6 or more merchant IDs will be discussed with you upon enrolment. You may be offered **Global Fortress** at a bespoke fee, dependent on your circumstances. To enjoy this, fees may be payable to SecurityMetrics annually in advance at the time of enrolment.

[2]**SecurityMetrics -** Whilst we appreciate that you may have expressed a no marketing option or registered with the telephone preference service, compliance with this mandate to become PCI compliant is essential if we are to continue providing you with a card processing service.

[3]**Administrative fee when choosing an alternative QSA or complete a SAQ -** Administrative fees start from £3.00 per merchant ID per month (plus VAT, where applicable) where no vulnerability scans are required. If vulnerability scans are required, you will need to use a QSA and our administrative fee is £6.00 per merchant ID per month (plus VAT, where applicable).

*SecurityMetrics is open for enquiries between 9am and 5pm Monday to Friday (excluding public holidays). Calls may be monitored and/or recorded.

**Lines are open between 9am and 5pm Monday to Friday 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.

Global Payments
51 De Montfort Street
Leicester
LE1 7BB
Tel 0345 702 3344
Textphone 0345 602 4818
www.globalpaymentsinc.co.uk

KTR 03/2019 | GP092