planet

Merchant Operating Instructions

For Acquiring Services

Contents

Welcome to Planet and thank you for selecting us as your acquirer.

These are your Merchant Operating Instructions. It is important that you and all of your staff are familiar with the procedures in this guide. You should read these instructions together with your Terms of Business and your Terminal User Manual.

This guide should cover the questions most frequently asked by Merchants, however, if you require further help or have any comments, please do not hesitate to contact your account manager or local technical support for assistance.

2. General Card Acceptance

This section focuses on card acceptance. For wallet acceptance please refer to Section 8.

Card Types - You can only accept cards from the Card Schemes detailed in your Terms of Business. If you process a transaction on a card from a scheme that you are not permitted to accept, the transaction will be rejected and returned to you.

Card Acceptance – Card payments are taken at your own risk. By following the instructions in this guide and your Terminal User Manual, the risk may be reduced, but it is important to understand that card payments are not guaranteed and can be charged back if disputed at a later date.

Use of your Terminal - You must only process transactions (purchases and refunds) that relate to the sale of goods or services provided by your business:

- Do not process transactions on your own card(s) or on cards belonging to a director or partner of the business card(s) e.g. to generate sales and turnover or to remove funds from the business.
- Never process transactions on behalf of third parties and do not allow any unknown party access to your terminal.
- Do not transmit or accept for payment any transaction that was not originated directly between your business and the cardholder.
- Do not initiate a credit transaction (refund) without there being sufficient funds in the settlement account or merchant bank account to meet the debit.
- Do not process a transaction in exchange for providing a cardholder with cash, unless this has been specifically approved as part of your payment services application.
- Do not split a sale into separate amounts on one card or across different cards to avoid obtaining authorisation for the full transaction amount.
- Do not use the software or any data received for any other purpose other than for determining whether or not you can accept cards in connection with a sale for the provision of goods or services.

Authorisation – Authorisation of a transaction is not a guarantee of payment. It means that at the time of the authorisation request, the card has not been blocked and that there are sufficient funds available on the card/card account at the time of the request to meet the purchase. Do not obtain authorisation for the purpose of setting aside a cardholder's credit line for use in future sales.

Nature of Goods/Services - If you change the nature of the goods or services your business supplies you must inform Planet in advance of processing any further card payments. This includes a change in the length of any guarantees or warranties offered on the products you sell.

Business Changes – You must inform us of any change in your business, such as a change in the type of legal entity, a change in ownership, directors or partners, a change of address/contact details or a change in bank account details. You must also inform us of any insolvency event (or impending insolvency event) or any actual or impending sale or other disposal of all or any material part of your business.

Submission of Transactions - Please note that the end-of-day batching process should be carried out using your terminal every day on which transactions are accepted to avoid any late presentation charges. You should submit the data captured on your terminal within three business days. Any transactions submitted after this time will be downgraded by the Card Schemes and may attract an additional charge.

Card Present Transactions

General guidelines for card acceptance are detailed below, but when carrying out a sale or refund using your terminal please refer to the Terminal User. Either your terminal or Terminal User Manual will advise you whether you or your customer inserts the card into the terminal or PIN Entry Device (PED).

In normal circumstances, card acceptance will be via Chip and PIN (personal identification number). However, some cardholders may still need to provide authorisation by way of signature. You must not refuse to accept these cards.

Chip & PIN Authentication

A customer must never disclose their PIN to you and they should be encouraged to shield the PIN Pad when entering their PIN. The general acceptance process for Chip and PIN transactions is as follows, but please refer to your Terminal User Manual for detailed procedures:

- The cardholder should insert their card into the Chip reader within the terminal or separate Pin Entry Device (PED). If you have a separate PED always keep it and the cardholder in sight throughout the transaction process.
- The terminal should then request the cardholder to enter their PIN. If it does not, follow the terminal prompts.
- Ask the cardholder to enter their PIN after they have checked the transaction amount is correct.
- The terminal will normally authorise the transaction automatically, however if it does not, follow the terminal prompts.
- When the terminal has printed the transaction receipt and you are confident that everything is in order, ask the customer to remove their card from the terminal

or PED and give them their copy of the receipt along with the goods they have purchased.

- The Transaction is now complete.

Incorrect or locked PIN: If the Cardholder enters the wrong PIN three times use of the card will be locked and they should be advised to contact their Card Issuer.

Faulty card: A terminal will usually attempt to read the data on a chip three times. If unsuccessful after three attempts, the terminal may default to a magnetic stripe transaction.

Signature Based Authentication

Only use a signature to verify a transaction when absolutely necessary. This occurs primarily when the card does not support Chip and PIN authentication or the cardholder is unable to use PIN verification. The general acceptance process for signature based transactions is as follows, but please refer to your Terminal User Manual for detailed procedures:

- Insert the card into the terminal, which will indicate that signature verification is required.
- Follow the terminal prompts.
- The terminal will normally authorise the transaction automatically but if it does not, do not proceed with the transaction and follow the terminal prompts.
- When the terminal has printed the transaction receipt, check that the card number, expiry date and card type (e.g. Visa or MasterCard) match those of the card. Also check the card for any signs of damage and that the gender of the presenter matches the title of the cardholder detailed on the card.
- If the details match, the card expiry date has not passed and you are confident that everything is in order, ask the customer to sign the terminal receipt.
- Check that the signature matches that on the signature stripe whilst also checking it for any signs of tampering. If you are happy it does, confirm the transaction on the terminal and hand the card back to the customer along with their copy of the receipt and the goods they have purchased.
- The transaction is now complete.

Card Not-Present Transactions

Card Not Present (CNP) transactions include the following:

- E-commerce - transactions processed through a secure online internet payment facility.
- Mail Order/Telephone Order (MOTO) - transactions processed through your terminal following receipt of an order via mail, telephone or fax.
- Recurring transactions.

CNP transactions present an increased fraud risk to you because there is no face-to-face contact with the customer and no sight of the payment card. These transactions are undertaken entirely at your own risk and you therefore need to be aware of the risks when accepting them. For example, MOTO transactions, if disputed, can be very hard to defend from chargeback because it is difficult to prove that the genuine cardholder placed the order/authorised the purchase.

E-commerce

If we offer E-commerce in your market and you wish to process E-commerce transactions your agreement with us must specifically state this and when in place you will have a specific E-commerce acquiring facility. If you are not using Planet as your Payment Service Provider (PSP) then your PSP should deal with the capture and processing of transactions on your behalf. In most cases the PSP will capture:

- Card number.
- Card issue number (if applicable).
- Cardholder name as it appears on the card.
- Card expiry date.
- Cardholder's full billing address, as it appears on their billing statement.
- Shipping/delivery address if different from the billing address.
- The three-digit Card Security Code (CSC) (also known as the CVV2), which appears at the end of the signature strip (if your PSP is capable of capturing this).

Website Requirements

You must include the following information on your website to make it easier for customers to shop online. This will reduce cardholder disputes and potential chargebacks.

- Your business - Your business and the permanent address of your establishment, including - company name, company registration number and VAT registration number.
- Customer Service - Customer service contact details, including phone number(s), e-mail address and postal address.

- Terms of Business – Clear details that establish what commitment the cardholder is being asked to make when purchasing goods/services.
- Goods/Services - A complete description of goods and services being sold, along with the total cost including any delivery, shipping and handling fees.
- Cancellation Policy – The rules by which a customer can cancel their order, including any specific deadlines and consequences of non-cancellation.
- Return/Exchange/Refund Policy – the rules by which a customer may return goods and/ or seek a refund or exchange.
- Delivery Policy - Including any restrictions on delivery e.g. export restrictions.

Verified by Visa, MasterCard SecureCode, UnionPay Secure Plus and similar systems

For E-commerce transactions, Cardholders can be authenticated by using Verified by Visa, MasterCard SecureCode and UnionPay Secure Plus, which together are also known as 3D Secure. These allow the customer to validate that they are the genuine cardholder at payment stage, by entering a unique password. This can assist in the reduction of and protection from chargebacks where the cardholder denies undertaking a transaction. Westrongly recommend that all merchants use 3D Secure and they should contact their PSP for further information.

Please note: If you wish to accept Maestro cards for E-commerce transactions, you must use MasterCard SecureCode.

Mail Order/Telephone Order (MOTO)

You must obtain the following information from the customer to process a MOTO transaction:

- Card number.
- Card issue number (if applicable).
- Cardholder name as it appears on the card.
- Card expiry date Cardholder's full billing address as it appears on their billing statement.
- Shipping/delivery address if different from the billing address.
- The three-digit Card Security Code (CSC) also known as the CVV2, which appears at the end of the signature strip (if your terminal is capable of checking CVV2 data).

You should then refer to your Terminal User Manual and follow the prompts on the terminal, which will detail the information required including how you can use the CVV2 and numeric characters within the cardholder billing address (Address Verification Service or AVS) to help validate the transaction.

CVV2 and Address Verification Service (AVS)

The CVV2 is a three-digit number printed on credit and debit cards and can usually be located at the end of the signature strip, on the reverse of the card. You can use this number to help validate a CNP transaction because the customer generally has to be in physical possession of the card at the time they place an order.

Note: CVV2 data must never be retained.

AVS checks the registered billing address given by the cardholder against the address held by the card issuer. This is undertaken by way of the numeric within the postal address e.g. house number and numbers within the postal code.

Please note that it may not be possible to undertake AVS checks on all addresses e.g. some overseas and even if CVV2 and AVS checks are unmatched, the transaction may still be authorised. It is your decision to accept or decline a transaction and even if a full match is given, this must not be taken as a guarantee of payment.

Recurring Transaction

Recurring transactions are designed as a way to collect regular payments (e.g. subscriptions or instalments) from your customer's card. You should complete the first transaction in the recurring transaction chain as securely as possible - Chip and PIN if the cardholder is present, or in the case of MOTO with CVV2 verification, you must not keep the CVV2 to process future payments.

You must not offer recurring transactions to your customers unless this has been specifically approved as part of your payment services application.

You must obtain written cardholder permission allowing you to take regular payments from their card and this should always be kept on file for the duration of the arrangement and a copy provided to the card issuer upon request. The information contained within the written authority, which must include a statement to the effect that it will remain in force until such time that it is cancelled in writing, should include:

- Card number.
- Cardholder name.
- Cardholder's full address.
- Cardholders telephone number.
- Payment pattern.

Note: Please remember that if you collect personal data of the customer, you must comply with all relevant data protection rules and regulations in your country. If you do not do this, we will not be responsible for any action that may be taken against you.

Cancelling Recurring Transactions

You must provide the customer with contact details in case they wish to cancel a recurring transaction and:

- Check for receipt of requests for cancellation or non-renewal of services paid for with a recurring transaction each day;
- Comply with all cancellation and non-renewal requests in a timely manner and notify the cardholder that the recurring payment has been cancelled;
- If you receive a cancellation request too late to prevent the most recent recurring charge from being posted to the cardholder's account, process a credit promptly and notify the cardholder accordingly.

Refunds

Please refer to your Terminal User Manual for guidance on how to process refunds as this will depend upon the type of terminal you have, however please be aware of the following:

- Only process a refund to the card on which the original transaction took place;
- Check that the card you are refunding was used in the original purchase by matching the last four digits of the card number to those printed on the original terminal receipt;
- Never refund by way of cash or cheque when the original purchase was made using a card and do not refund a card where the original payment was by other means e.g. cash or cheque; and
- If your terminal requires a supervisor card or PIN to enable the processing of refunds, please make sure that this is controlled by an authorised individual.

3. Fraud Prevention/Best Practice

Staff and Staff Training

Know your staff – Obtain and check references for all staff hired, including temporary and short-term cover. Ensure your staff have the appropriate authority to undertake transactions, including sales, reversals and refunds.

Training - You must provide appropriate training for staff so they are able to recognise suspicious cardholder activity and/or orders – they are your first line of defence against fraud. You should adopt in-house procedures so that staff know what to do if any such activity is identified.

Access to Your Terminal

Do not allow an unknown individual access to your terminal and do not accept an unexpected "replacement" terminal in exchange for your existing one. If you receive an unsolicited approach in this respect from any individual claiming to represent Planet or its partner, a sales agent representing Planet or your terminal supplier, never allow them access to your terminal without having independently validated who they are, by for example, contacting us using a phone number or e-mail address already known to you and not one provided by the individual.

Terminal Problems or Errors – Unsolicited Contact

If you receive an unsolicited phone call (or visit from any individual) asking that you call a specific phone number to obtain authorisation for every transaction due to issues with your terminal, do not act upon this.

If you receive a call and are asked to supply details of previous transactions because they were not processed correctly/successfully due to an alleged processing error, do not reveal any card or transaction details. Fraudsters are known to use these tactics in order to obtain card information.

Do not act upon any phone instructions that ask you to process "test" transactions, specifically refunds, which are claimed to be required to resolve an alleged issue with the terminal that is unknown to you. If you process a refund of this nature the funds will be paid to the card and debited from your bank account.

Technology Maintenance

- Make sure all Terminal device wiring is secure and not accessible to the public or unauthorised members of staff.
- Make regular checks to monitor that no additional recording or key capture devices are present on the site, e.g. in ceiling panels attached to laptops or charity boxes.
- Make sure surfaces around the till area are clear so that any unauthorised attachments or recording devices can be easily identified, including mobile phones.
- Complete regular checks on all equipment to ensure that no tampering has taken place.

Card Present Transactions

Always use Chip and PIN authentication whenever possible as this is the most secure way for you to accept transactions. Never process a transaction by swiping the magnetic stripe or by keying in the card number, known as PAN-key entry (PKE), just because the cardholder cannot remember their PIN and always:

- Follow all terminal prompts;
- Keep the terminal in sight during each transaction and recover it from the customer as soon as they have entered their PIN;
- Be aware if a customer tries to distract you whilst the transaction is being undertaken, especially during the authorisation stage, as they may be trying to prevent you from noticing a problem with the authorisation;
- If an authorisation code has been manually entered into the terminal, it will state that on the receipt. If you are suspicious of a customer's behaviour with the terminal, you should check the receipt before completing the sale. If a manual authorisation code has been entered, you must cancel the transaction and complete a new transaction.
- Be aware of 'out of the ordinary' purchases e.g. the bulk purchase of random goods or of clothes in varying sizes. Most customers take care when making a purchase and try clothing on, whilst a fraudster is more likely to be careless and hasty and will look to buy goods that they can easily re-sell.

If transactions are undertaken by way of magnetic strip and signature or PKE make sure that:

- The security features on the card are present and correct;
- The signature strip has not been tampered with or that another strip has not been placed over the top of the original;
- The signature appears original. If the word 'void' appears on the strip, it may indicate that the original signature has been removed. If the signature is in felt-tip pen it may be over-writing the original, which should be in ballpoint pen;
- The cardholder's signature matches that on the card;
- The gender of the card presenter matches the title on the card; and
- The last four digits of the card number on the receipt match those on the front of the card.

Card-Not-Present Transactions

Given the increased risk posed by CNP transactions, you and your staff should be aware of the warning signs that may indicate that a transaction or transactions may be fraudulent:

- Unmatched CVV2 and/or AVS data - consider undertaking additional checks to verify the transaction and/or rejection of it;
- Multiple orders on the same or different card numbers from the same customer;
- A first-time customer who places multiple or high value orders – known customers are clearly of lower risk;
- The purchase of high volumes of goods which are easy to re-sell and desirable, for examle electrical equipment (televisions, computers, mobile phones), and jewellery;
- Multiple orders on cards that contain the same first six digits (BIN), especially if one or more of the card numbers is declined and an alternative offered immediately afterwards;
- Multiple transactions on various different cards, from either the same or different customers, where the goods are to be delivered to the same address;
- A request for urgent delivery when any additional delivery costs are of no concern to the customer;
- An out of the ordinary purchase where delivery is to an overseas address – if overseas orders are unusual, take time to consider why this customer has chosen your business;
- Orders where the delivery address is different to the billing address, especially if the delivery address is for example a PO box or hotel;
- A request to hand goods over to a third party e.g. a taxi driver, courier, messenger or chauffeur sent by the customer to collect them.

Within the E-commerce environment, also look out for:

- Any alert from your PSP that may indicate that the transaction is of higher risk;
- The same IP address being used by multiple customers e.g. orders originating from the same IP address but with different shopper names and e-mail addresses;
- Orders where the cardholder billing country, IP country and card issuer country do not match;
- An e-mail address that bears no resemblance to the shopper name, or where the shopper details (e-mail, name, address) are illogical or fictional characters;
- Multiple transactions being attempted by one shopper on multiple cards;
- Card testing – where multiple transactions are attempted on cards that appear to run in close sequence.

Minimise the risk of becoming a victim of CNP fraud by always following these guidelines and making use of the security tools available. For MOTO transactions use CVV2 and AVS checking and for E-commerce transactions also offer cardholder authentication through Verified by Visa, MasterCard SecureCode and UnionPay Secure Plus.

If suspicious, take steps to further verify your customer's identity. Try contacting them using the contact details (e-mail and phone number, a landline is preferable) that they have given you.

Always try to deliver goods to the individual who placed the order and to cardholder's billing address, do not hand goods over to someone waiting outside. Obtain a signature from the cardholder as proof of delivery and keep this with your transactional records in case a dispute arises.

You may also wish to consider screening your transactions to identify those that are of higher risk. It may be possible for you to do this this in-house through transaction velocity checking and through use of previously reported fraud and/or chargeback data. For example, if an order comes in and goods are requested to be delivered to an address which has been linked to previous transactions that were subject to chargeback, why deliver to it again without undertaking additional checks?

Alternatively, your PSP may offer a fraud screening service or you may wish to consider using third party transaction screening tools.

Please remember that if at any stage the cardholder decides that they want to collect the goods from your business, they must attend in person and produce the payment card. You should then reverse, cancel or refund any previously completed CNP transaction and process a new cardholder present transaction.

Common Fraud Types

Additional Funds Transfer

Do not agree to send additional funds to a customer following a sale by any means. The following fraud method has been observed in recent years:

- When completing a sale, a large deposit or full payment will be made to purchase your goods/service.
- A few days after the booking, the customer will contact you to inform you that they are using a third party for additional or value-added services e.g. car/coach hire or interpreter.
- The customer will then request for you to transfer funds directly to the third party's bank account to cover the costs of the third-party services.
- All contact with the customer will be lost once the funds are received in that account.
- The transactions will eventually be charged back by the genuine customers and you will be responsible for paying these, as well as being left out of pocket for the additional funds transferred.

Transaction Refund via Alternative Means

If a customer requests a refund, it is important that you process the refund onto the same card used for the original purchase and do not refund them via alternative means. Typically:

- A customer purchases a high-value item and then informs you that they have changed their mind.
- They then request you to provide a refund to a different card or via a wire transfer to their bank account.
- A chargeback for 'credit not processed' will be raised by the customer and you will usually be unable to defend this by saying you had refunded the customer via alternative means.
- In all instances, you must attempt to process a refund to the card used for the original purchase. If the card used for the original purchase has expired, it is normally still possible to refund the account and the Card Issuer will transfer the funds to the customer's new card. If this is not possible, please follow the prompts on your terminal.

Use of Damaged Cards

When processing a transaction, it is important that you do not accept a card that has been damaged. Look out for the following:

- When a card is inserted into your Chip & PIN device, the terminal displays a message advising that the card cannot be read and/or the magnetic stripe is damaged.
- The customer will then suggest you manually enter the card number into your terminal. This may either be taken from the front of the card or may be given to you by the customer themselves.

If you are presented with a card that is clearly damaged or your terminal cannot read the details, do not accept the card and suggest the customer speaks to their card issuer to obtain a replacement card.

Insist that the customer uses an alternative form of payment to complete the sale.

Third Party Processing

As part of your agreement with us, you must only provide the goods/services you informed us about during your application and must only use your facility for your own business' operations. Another common fraud type is as follows:

- An individual, group or business will contact you and will offer a 'lucrative opportunity' if you agree to process transactions on behalf of a third party through your Planet merchant facility.
- You will be instructed to transfer the funds for these third-party transactions to a specific bank account and will receive a portion of the funds in return.
- As the transactions will have been processed by your business, you will be responsible for any chargebacks or Card Scheme assessments that result from these.
- It is very likely that these transactions will be for illegal or high-risk goods/services, so the implications can be very serious.

If you believe you have been targeted by one of the above fraud types, or believe someone is impersonating a Planet employee/department, please report this to our fraud team using the following email address:

investigations@planetpayment.com

4. Disputed Transactions and Chargebacks

Chargebacks

A chargeback is the means by which a card issuer can reclaim funds on behalf of a cardholder in respect of a transaction that has been processed by a merchant.

This may occur if the cardholder or card issuer disputes the validity of a transaction. When a transaction is disputed the card issuer and Planet operate to clearly defined Card Scheme regulated procedures to manage the dispute and establish whether funds should be retained by the merchant or returned to the cardholder.

Why Do Chargebacks Occur?

A Chargeback can occur when there is a dispute over the validity of a transaction, goods/services have not been supplied or when there has been a processing error. Some of the most common reasons for receiving a chargeback are:

- Failure to respond to a retrieval/copy request within the stated timescales, or with appropriate information;
- The cardholder claims their card has been used fraudulently, without their knowledge or without their specific authority;
- The original transaction required authorisation but this was not obtained;
- The cardholder does not recognise the transaction from the information on their statement, such as the amount, the merchant 'doing business as' name or the location;
- A service or recurring transaction authority has not been cancelled, despite the cardholder's request to do so;
- The cardholder was promised a refund and did not receive one;
- A cardholder has been billed twice for the same purchase;
- There has been a mistake in the processing of a transaction; or
- The cardholder has not received of the goods; the expected service has not been supplied or the quality of the goods/service is different to that advertised.

You have the right to dispute a chargeback and to do so you will need to supply us with information and evidence to prove that the transaction was authentic, authorised and undertaken by the genuine cardholder. We will consider any information you supply and attempt to dispute the chargeback when appropriate, but cannot guarantee this will be successful and will ultimately depend on whether the evidence provided meets the requirements set out by the Card Schemes.

Chargeback and Copy/Retrieval Request Process

A Chargeback or Copy/Retrieval Request (also known as a Request for Information or RFI), is a request for transaction information e.g. a copy of a voucher or proof of a cardholder's participation in the transaction.

Copy/Retrieval Requests are not necessarily a mandatory stage of the dispute process and a Card Issuer can raise a Chargeback without initiating a Copy/Retrieval Request.

When information in respect of a transaction is requested, you will receive either a Chargeback notice or a Copy/Retrieval Request notice via email from your local Planet office. You have seven days to respond to the Copy/Retrieval Request notice and ten days to respond to the Chargeback notice. If the Copy/Retrieval Request is not acted upon within this period, the issuer can raise a Chargeback and your account will be debited for the disputed transaction amount.

In response to a Chargeback or Copy/Retrieval Request, you must send a legible copy of the requested receipt or file along with any other transaction information you have to your local Planet office. If Copy/Retrieval Requests are incompletely fulfilled or not fulfilled within the specified time limit, this will invariably lead to a Chargeback due to 'non-fulfilment of Copy Request'. The transaction receipt and/or additional documentation should contain all the information available about the transaction, such as, but not limited to:

- Card number (the first 6 and last 4 digits only).
- Card expiry date.
- Transaction amount.
- Transaction date.
- Transaction Currency.
- Authorisation code.
- Merchant name.
- Description of the goods or services/merchandise or services sold.
- Merchant contact information/Merchant Location (On Line Address).
- Cardholder name and address (primarily for MOTO and E-commerce transactions).
- Billing address.
- Shipping address.
- Address verification response code.
- Cardholder telephone number or email address.
- Proof of delivery.
- For recurring transactions, a copy of the written cardholder authority.

Avoiding Unnecessary Chargebacks

While disputes are rare for most merchants, they are probably inevitable at some point in time. Not dealing with them adequately can lead to Chargebacks, which in turn can result in loss of business and revenue. To minimise losses from Chargebacks, you must understand your responsibilities in the Chargebacks process and establish procedures and practices for managing them.

The following guidelines will help in preventing chargebacks:

Fulfil copy requests - Always supply copy documentation to respond to Copy/ Retrieval requests as soon as possible. Send legible copy documentation with all necessary and available information in respect to the transaction within the specified time limit. Incomplete or unfulfilled requests will invariably lead to a Chargeback due to 'Non-fulfilment of Copy Request'.

Recognisable merchant name - It is critical for customers to be able to recognise transactions on their card accounts/statements to avoid potential disputes and Chargebacks for 'Cardholder Does Not Recognise'. The name under which you trade and the one that is visible to the customer when they purchase goods from you should be the same on the receipts provided to cardholders and the information shown on their account/statement.

Expired card - If the card expiry date given by the cardholder precedes the transaction date, the card is expired and is invalid. If you do not obtain authorisation, the transaction may be charged back as 'Expired or Not Authorised'. Note: A card is valid until the last day of the month indicated on the card. For example, 'Valid until 04-22' means the card is valid until the 30th day of April, 2022, but expires on May 1st, 2022.

Declined authorisation – A transaction should not be completed if the authorisation was declined. Similarly, in the case of 3D Secure transactions, the merchant should not proceed where the authentication has failed.

Submit transactions only once - Make sure transactions are deposited and files are transmitted only once. If the same transaction is processed more than once it will lead to a chargeback due to 'Duplicate Processing'.

Communicate your return, refund and cancellation policies - If you have return, refund and cancellation policies in place, communicate these clearly to the cardholder at the time the transaction is completed, or include this information in clear terms on your website and adhere to them.

Transaction receipt deposits - It is always beneficial for the merchant to deposit or submit transaction information for processing as soon as possible, preferably within a period of one to three days from the transaction date. Submitting information after this period may lead to chargebacks due to 'Late Presentment'.

Deposit or submit refunds (credit transactions) quickly – We suggest you process refund transactions as soon as possible, preferably the day it was generated. If refunds are not processed to cardholder accounts quickly, this may lead to the receipt of Chargebacks for 'Credit Not Processed'.

Customer complaints - Act promptly when a cardholder contacts you about a problem. You may be able to avoid a Chargeback for the likes of 'Goods and Services Not as Described' if you address customer complaints promptly.

Delayed Delivery - If the merchandise or service to be provided to the customer will be delayed, notify the customer of the delay and the new expected delivery date. This will help avoid a chargeback due to 'Non-receipt of Merchandise' or 'Services Not Rendered'.

Out of Stock Merchandise - If the merchandise requested by the cardholder is not in stock, or the merchandise is no longer available, notify the cardholder and offer the option to acquire similar merchandise or cancel the transaction. To avoid a potential chargeback due to 'Not as Described' or 'Non-Receipt', merchandise should not be substituted without the customer's agreement.

Ship goods before processing transactions – You must not submit transactions for processing until the ordered goods has been shipped (a deposit payment for goods is the exception). If the customer sees a transaction on their statement before the goods are received, this may lead to a chargeback for 'Non-Receipt of Merchandise'.

Recurring transaction cancellation requests - If the customer requests the cancellation of a transaction that is periodically billed (monthly, quarterly or annually), it is important to always respond to the request and cancel the transaction immediately or as specified by the customer. Confirm to the customer in writing that the request has been received and completed. Failure to respond to cancellation requests will almost invariably lead to a chargeback.

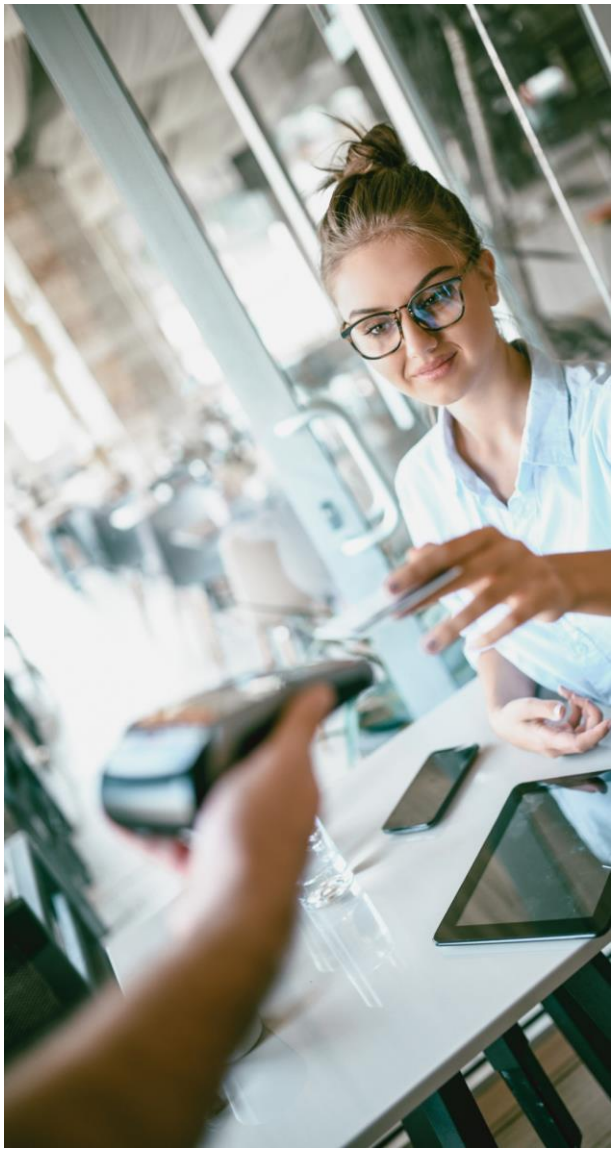
5. Settlements, Fees, Collaterals (Bank Details)

Settlement type – We offer net and gross settlements to merchants. Net settlement involves settling net of our charges agreed in the Planet application form. Merchants receive statements with a summary of all transactions included in the settlement.

Currencies – You will enjoy the benefits of receiving settlements in the currency assigned to your bank account in your home country or the location in which your business is transacted. You should send requests for receiving settlements in additional currencies to your account manager.

Transaction Fee – This is the previously agreed transaction fee from each transaction that goes through the settlement process. Transactions that have been authorised but were never settled are also subject to these fees.

We reserve the right to introduce new fees subject to applicable regulatory requirements.



6. Payment Card Industry Data Security Standard Requirements

What is PCI DSS?

The Payment Card Industry (PCI) Data Security Standard (DSS) is a comprehensive set of international security requirements to help protect cardholder data. The PCI DSS was developed by Visa and the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS consists of twelve basic requirements. These requirements are the foundation of data security compliance programme known as the Account Information Security (AIS) Program.

All acquirers and card issuers must comply, and must also ensure the compliance of their merchants and service providers who store, process, or transmit credit card account numbers. This programme applies to all payment channels including card-present, mail/telephone order, and E-commerce.

By complying with PCI DSS requirements:

- You build consumer trust in the security of sensitive information.
- Customers seek out merchants that they feel are "safe." Confident consumers are loyal customers. They come back again and again, as well as share their experience with others.
- You minimise direct losses and associated operating expenses.
- Appropriate data security helps protect cardholders, limit risk exposure, and minimise the losses and operational expense that stem from compromised cardholder information.
- You maintain a positive image for card payment services.
- Information security is on everyone's mind, including the media. Data loss or compromise not only hurts customers, it can seriously damage a business's reputation.

For additional information about the PCI DSS please visit:

https://www.pcisecuritystandards.org/merchants/

https://www.eiseverywhere.com/ehome/index.php?eventid=8231&tabid=17737

http://www.visaeurope.com/en/businesses__retailers/payment_security.aspx

Sensitive Data Storage and Payment Application Use

All stored, processed or transmitted sensitive cardholder account or transaction information must comply with the PCI DSS. To protect sensitive customer and transaction information from compromise if you

store, process, or transmit cardholder account or transaction data you must:

- Keep all material containing account numbers - whether on paper or electronically - in a secure area accessible to only selected staff. You should be extremely careful in storing and transferring sensitive information if you use paper receipts. You should:
  - Promptly provide the drafts to your acquirer.
  - Destroy all copies of the drafts that are not delivered to your acquirer.
- Make sure cardholder data is unreadable, both in storage and before you discard it.
- Never retain full-track, magnetic-stripe, CVV2 and chip data (Sensitive Authentication Data – SAD) after a transaction has been authorised. Storage of track data elements in excess of name, personal account number (PAN), and expiration date after transaction authorisation is strictly prohibited.
- Never disclose any information obtained through the software to any person except for necessary disclosures to affected cardholders, and/or the Card Schemes or Card Issuer.
- Use payment applications that comply with the PCI Payment Application Data Security Standard (PA-DSS). A list of validated payment applications is available at www.pcissc.org

Account Data Compromise

You must report immediately any occurrence that results in the unauthorised access to or disclosure of sensitive cardholder account or transaction information.

You should also be aware of your obligations in respect to any Account Data Compromise Event as set out in MasterCard Security Rules and Procedures:

http://www.Mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf

Merchant Third Party Agent Registration

Third Party Agents are service providers that assist you in the delivery of a payment service. For example, a solution provider that provides an E-commerce gateway.

Any third-party agent that you use must be validated for PCI DSS compliance and listed on Visa's validated service providers list. The global list of PCI DSS Validated Service Providers is located on https://www.visamerchantagents.com/.

Planet Merchant Services Merchant PCI DSS Compliance Service

For Planet Merchant Services to ensure and report on merchant PCI DSS compliance, merchants must complete the Planet PCI DSS service registration and annual compliance attestation. This is a two-part process, where part 1 requires merchants to register their payment set up and configuration, and part two where merchants answer a series of questions ("Information Security Policy") to confirm their PCI DSS compliance.

As part of the merchant onboarding process, merchants will receive an email from Planet Merchant Services with instructions and a link to the service portal.

The service has been designed to be as user-friendly as possible, helps merchants manage their PCI DSS compliance, and offers value-added services such as the ability for the merchant to schedule vulnerability scans.

Participation and completion of the Planet PCI DSS service is mandated for Planet Merchant Service acquired merchants. Planet operates an Escalation Process whereby reminder emails and prompts are issued to merchants who have not fully completed the process.

As part of the use of the Planet PCI DSS service, merchant is mandated to operate an anti-virus software programme to protect the service and portal from unintentional uploading of any disabling devices and/or Trojans.

Other Information

Retention of Documentation:

You must keep copies of your sales and refund transaction receipts and any additional information in respect to them, such as order forms and proof of delivery, in a safe and secure place for at least 18 months. These documents may be required in the case of a cardholder or card issuer dispute and might be requested through a retrieval request, copy request or chargeback. If you destroying documentation after 18 months, be sure to do so in a secure manner.

Advertising / Point of Sale Display:

If you wish to advertise in the press or other media to show that you accept cards as a method of payment, the following rules apply:

- The Card Scheme logos have been registered as trademarks and must be used in accordance with instructions issued and available from the Card Schemes.
- The Card Scheme logos must not be featured in advertising in a manner where endorsement of the goods and/or services being offered by you, is given or implied.
- Card decals/stickers are provided to all retailers. These must be clearly displayed in your outlet(s).

Once displayed, you cannot refuse to accept a Card Transaction.

Change of Bank Account Details:

Please tell your account manager if you change your nominated bank account.

Change of Ownership/Status/Name/Address:

Please tell your accu9nt manager immediately if your business (or any of its outlets) changes ownership, status, products sold and/or services supplied, name or address If you do not we may have to suspend services.

7. Card Recognition Guide

When dealing with cardholder present transactions, in the majority of circumstances it is unlikely that you will be required to handle a customer's card given that most transactions will be processed as Chip and PIN. However, it is still important that you understand and recognise the security features that should appear on a card if it becomes necessary to validate the card and customer through other means, such as magnetic swipe and signature.

Front of Card

There are various different Visa, MasterCard and UnionPay card designs, including some with a vertical card orientation as opposed to the more familiar horizontal design. Some cards may not be embossed with a full card number or cardholder name, but valid cards will contain a card scheme logo, hologram, ultraviolet image and card security code (also known as CSC or CVV2).

1 Chip – not all cards contain a Chip and if not, you can still accept transactions using the magnetic stripe.

2 Primary Account Number (PAN) – this can be embossed or flat printed. Visa cards start with a 4 and MasterCard cards with either a 5 or 6.

3 First four digits – these four digits will be flat printed underneath the Primary Account Number and should be identical to the first four digits of it.

4 Cardholder name – embossed cards should have a cardholder name, company name or a generic description such as gift card, travel card, club member.

5 Expiry date – all cards have an expiry and some, not all, have a valid from date.

6 Contactless indicator – the 'wave' symbol indicates the card can be used for contactless payments that don't require the card to be inserted or swiped.

7 Card Scheme logo – the following MasterCard, Visa or UnionPay logo should appear on the front:

Reverse of Card

8 Card Scheme Hologram – the following Card Scheme holograms should be present. On some cards this may appear on the front and if so generally on the right-hand side at the end of the Primary Account Number.


Visa


Mastercard


UnionPay

9 Magnetic Stripe – stripe containing card information in a magnetic format.

10 Signature Strip – the signature stripe should be flush with the card surface and will either have 'Visa', 'MasterCard' or 'UnionPay' printed on it. The full card number (Primary Account Number) or the last four digits of it should also be printed in reverse italic text on the signature strip.

11 Card Security Code – always shown on the reverse of the card, either on the signature strip or within a white box to the side of it.

Ultraviolet Image

Visa and MasterCard cards also contain security features, which can only be seen under ultraviolet light, whereas UnionPay has no ultraviolet image.

For Visa cards, an ultraviolet 'V' can be seen within the Visa logo, as shown in the below image, whilst the word 'Visa' is also repeated within the signature strip:

MasterCard cards contain ultraviolet letters 'M' and 'C' within the card in the areas indicated in the following image:

8. Wallet Acceptance

All terms, conditions and requirements set out in these instructions apply to wallet acceptance. Those elements that differ for wallet acceptance are listed in this section.

Wallet Types – we offer acceptance of AliPay and WeChat Pay wallets. You can only accept payment by wallets detailed in your Terms of Business.

Point of Sale Acceptance Solutions – we offer two acceptance solutions, a stand-alone tablet application and a payment terminal solution. You will initiate the transaction, but depending on the solution / terminal type:

- you will either need to scan the customer's QR code on their wallet application.
- or the QR will be displayed on your device for the wallet holder to scan to accept the transaction.

A confirmation message is then delivered to both your device and the wallet holder's mobile phone confirming success or failure of the transaction.

E-commerce – we offer a Pay By Link solution allowing you to generate a QR code allowing the customer to scan it on his wallet application to perform a payment.

Mail Order / Telephone Order (MOTO) – Alipay and WeChat Pay do not support MOTO transactions.

Recurring transactions – Alipay and WeChat Pay do not support recurring transactions.

Refunds – Please refer to your Terminal User Manual for guidance on how to process a refund on for a wallet transaction. Please note all refund transaction requirements that apply to card refunds also apply to wallet refunds.

9. Glossary

A

Acquirer – A financial institution that provides facilities to businesses to allow them to accept card payments.

Address Verification Service (AVS) – A process that checks the card billing address, provided by a cardholder during card not present sales, against the address records held by their card issuer. The check is undertaken by way of matching the numeric elements of the postal address.

Authorisation – Confirmation from the Card Issuer that the Cardholder has sufficient funds available for the Transaction and that the Cardholder's Card has not, at the time of the confirmation is requested, been blocked or reported lost or stolen.

Authorisation Code – A code that is generated by a card issuer, or by an acquirer on behalf of a card issuer, when an authorisation request is approved.

B

Batch – A collection of transactions from a terminal or merchant outlet e.g. a batch may refer to a single day's transactions.

BIN (Bank Identification Number) – The first six digits of a payment card number, which can be used to identify which financial institution has issued the card - the 'Card Issuer'.

C

Card Issuer – An organisation that issued a payment card to the cardholder.

Card Not Present Transactions (CNP) – Card transactions processed when the cardholder and card were not present with a merchant – e.g. mail order, telephone order and E-commerce transactions.

Card Number – The number shown on the front of the payment card (generally 16 digits but may be longer).

Card Present Transactions – Card transactions processed when the card and cardholder are present with a merchant during a transaction – Chip & PIN and magnetic stripe read are examples.

Card Schemes –Visa and MasterCard or UnionPay or any other card scheme notified by us to you from time to time.

Card Security Code (CSC) – The three-digit code at the end of the signature strip or in a separate white box next to the signature strip on the back of a payment card. American Express cards have a four-digit CSC on the front of the card. May also be referred to as CVV2. This code may be requested when Card Not Present transactions are being undertaken as it can be used to help validate the card being presented.

Card Verification Value (CVV2) – The three-digit code at the end of the signature strip or in a separate white box next to the signature strip on the back of a payment card. American Express cards have a four-digit CVV2 on the front of the card. May also be referred to as Card Security Code (CSC). This code may be requested when Card Not Present transactions are being undertaken as it can be used to help validate the card being presented.

Cardholder – The individual to whom a card is issued, or an individual authorised to use the card.

Cardholder Authentication – A term used in the E-commerce environment when a cardholder is being authenticated through Verified by Visa or MasterCard SecureCode, jointly referred to as 3D Secure.

Chargeback – The term used where a card issuer can charge part or all of the value of a transaction back to a merchant via their acquirer, for example, when a transaction is disputed because it is proven to be fraudulent or because the merchant has not followed the correct procedures.

Chip & PIN – Cards with Chip & PIN technology have a computer Chip embedded in the card, and the cardholder has a personal identification number (PIN) linked to the card, which should only be known to them. When the card is used to undertake transactions in a face-to-face environment through a Chip and PIN enabled terminal, the card is verified as authentic by the customer entering their PIN.

Copy Request - A request by either the card issuer or the cardholder wishing to obtain further information about a particular transaction.

Credit Card – A payment card linked to an account which has a credit or spending limit. The cardholder can usually pay off the entire outstanding balance by a set date, or can repay part of the outstanding balance subject to a minimum monthly amount. Interest will then usually be charged on any outstanding amount.

D

Data Compromise – An incident involving the breach of a system or a network where sensitive cardholder data is stored e.g. card number, cardholder name, card expiry date and cardholder address.

Debit card – A payment card, such as a Visa Debit, Mastercard Debit or Maestro card that is generally linked to a bank account and enables the cardholder to purchase goods/services with payment being debited to the bank account.

E

E-commerce Transaction – A transaction conducted via a computer and processed through a secure online internet payment facility.

Escalation Process - A process linked to the Planet PCI DSS service design to prompt and remind non-complying merchants to complete the Information Security Policy and attain their PCI-DSS accreditation. As part of this Escalation Process, Planet reserves the right to terminate the acquiring contract for non-complying merchants.

F

Fraud Screening – Additional analysis of transactions, primarily CNP, with the aim of identifying and preventing potential fraudulent card activity and reducing/preventing subsequent chargebacks.

Fraudulent Transaction – A transaction processed on a payment card that is subsequently disputed by the genuine cardholder as not having been undertaken or authorised by them.

H

High Risk Registration Fee – Planet is required to register merchants dealing in certain 'high risk' services in the MasterCard Registration Programme, for which a fee is levied.

I

IP Address – An Internet Protocol Address is the unique numerical label assigned to a computer participating in a computer network that uses Internet Protocol for communication. The two principle functions served by the IP address are: network interface identification and location addressing.

ISO – International Organisation for Standardisation publish a series of best practice recommendations on information security management, including risks and controls in this respect.

M

Magnetic Stripe – The data stripe on the back of a payment card that contains encoded information about the card and cardholder in a magnetic format. The magnetic stripe can be used for authorising a transaction in a card present environment when Chip and PIN is not used or is not working.

Mail Order/Telephone Order (MOTO) – A card not present transaction, where the card and cardholder details are captured from mail, fax or telephone interaction with the cardholder.

MasterCard Registration Programme (MRP) - Merchants who are involved in the provision of services that are deemed by MasterCard to be 'high risk' must be registered in the MRP. Services currently include: Telecommunications, E-commerce Adult Content, non-face-to-face Gambling, non-face-to- face Prescription Drugs and non-face-to-face Tobacco.

MasterCard SecureCode – A method introduced by MasterCard to provide an additional, secure cardholder verification process prior to an E-commerce transaction proceeding over the Internet.

Merchant – A business to whom card acquiring facilities are granted and used to process card payments in respect to goods/services purchased by and supplied to their customers.

Merchant Number – The unique number you are given when you sign a contract with us which identifies your business on our systems. This is also known as the Merchant Identification Number (MID) or Merchant ID.

Merchant Operating Instructions – The instructions in this guide.

P

PAN Key Entry (PKE) – The process of undertaking a transaction by keying a card number (primary account number) into the terminal or PED as opposed to using the Chip or magnetic stripe to capture the card details.

Payment Card – Generic term used for any plastic card (credit, debit, pre-paid, purchasing, etc.) that can be used to purchase goods/services or withdraw cash.

Payment Card Industry Data Security Standard (PCI DSS) – A compliance requirement that aims to ensure that cardholder information is always stored, processed and transmitted securely.

Payment Card Industry Security Standards Council (PCI SSC) - An organisation founded by five global payment brands – Visa, MasterCard, American Express, Discover Financial Services and JCB International.

Payment Gateway – The E-commerce equivalent to a point of sale terminal. The payment gateway facilitates the transfer of information between the cardholder, merchant and payment processor in a secure environment.

Payment Service Provider (PSP) – A PSP gives a merchant the means to accept and process online transactions on cards and other payment methods in the E-commerce environment. The PSP connects to an acquirer, or multiple acquirers and payment networks.

Personal Identification Number (PIN) – A number, generally of four digits, which is used to authenticate chip card transactions at the point of sale, or cash withdrawals and instructions initiated by a payment card through a cardholder-activated terminal, such as an ATM.

PIN Entry Device (PED) – An electronic device used in PIN based transactions to accept and encrypt the cardholder's PIN. Usually used in conjunction with integrated point of sale devices in which an electronic cash register/till is used to manage the sale and the PED is used to securely capture, encrypt and verify the PIN.

Primary Account Number (PAN) – The cardholder number of up to 19 digits, which is encoded on the card's magnetic stripe and usually, although not always, embossed on the front of the card.

Q

Qualified Security Assessor (QSA) – Organisations trained on PCI DSS by the PCI Security Standards Council that can confirm a merchant's compliance status, or offer support in reaching compliance. A list of qualified assessors is maintained by the PCI Security

Standards Council and can be found here: www.pcisecuritystandards.org.

QR code - (abbreviated from Quick Response code) is the trademark for a type of matrix barcode (or two-dimensional barcode) and is a machine-readable optical label that contains information about the item to which it is attached.

R

Recurring Transactions – A convenient way to collect regular payments, such as subscriptions or instalments, from customers' cards.

Request for Information (RFI) – A request by either the card issuer or the cardholder wishing to obtain further information about a particular transaction.

S

Sensitive Authentication Data (SAD) – Defined as full magnetic stripe data, CAV2/CVC2/CVV2/CID and PINs/PIN blocks – this data should not be retained by the merchant.

Service Provider – Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission and switching of transaction data, cardholder data or both.

Settlement – A transfer of funds to complete one or more transactions.

Split Sale/Transaction – When the customer pays part in cash and part by card. Never allow a customer to split the cost between two cards or two amounts on the same card in order to avoid authorisation for the full amount.

T

Terminal - The device provided by Planet, or the device used by the merchant to execute a software or an application provided by Planet or a software or an application provided by a third party and certified with Planet

Terminal ID – Unique number that is assigned for each terminal when you receive an acquiring facility from us, which identifies each terminal within your business and the transactions they process within our systems.

Terminal Receipt – The paper receipt that is printed out by the terminal when a transaction is completed. The customer is given one copy and the second is retained by the merchant and may be requested if a subsequent dispute or query is received in respect of the transaction.

Terminal User Manual – The instructions that came with your terminal and detail, amongst other things, exactly how to process transactions correctly. The guide should be read and understood by any member of your staff who processes transactions in conjunction with these Merchant Operating Instructions.

Track Data – Information about the card and cardholder that is kept in the card's magnetic stripe or chip. (See also 'Magnetic Stripe Data'.)

Transaction – A card payment in exchange for goods or services.

Transaction Amount – The full amount the customer pays for the goods or services, including any VAT.

Transaction Data – Information that identifies the purchases a cardholder makes with their card.

V

Verified by Visa (VbV) – A method introduced by Visa and the banks to provide an additional, secure cardholder verification process prior to an E-commerce transaction proceeding.

Vulnerability Scan – Externally-facing scans of your Internet-facing IP addresses that check for unknown vulnerabilities in your network.

W

Wallets – Financial accounts that allow users to store funds and make transactions.

Written Authority Form – The form your customer needs to complete to authorise you to take recurring transactions from their card. Find out more in Recurring Transactions.