AIB Merchant Services

AIB Merchant Services
Merchant Procedure Guide

Call us today on 0845 301 5407 • www.aibms.co.uk

AIB

Table of Contents

Welcome

Welcome to the AIB Merchant Services Merchant Procedure Guide. We would like to take this opportunity to thank you for selecting AIB Merchant Services for your Card acceptance services. AIB Merchant Services is one of Ireland's largest providers of card payment services, with operations in the Republic of Ireland, Northern Ireland and Great Britain.

We are a joint venture between Allied Irish Bank, p.l.c., and First Data Corporation, a global leader in electronic commerce and payment services.

Our relationship with our customers is at the heart of our business strategy. We are committed to offering the best service, products and delivery methods to ensure our customers have a first-rate payment solutions service.

This Merchant Procedure Guide contains important information about the services we offer along with the procedures Merchants must follow when processing Card payments.

This guide constitutes an integral part of your Agreement with AIB Merchant Services, as defined in the Terms and Conditions of Use (see www.aibms.co.uk for a copy of our Terms and Conditions) and the Glossary herein, for the provision of AIB Merchant Services facilities.

Therefore, it is important that:

- You read this Merchant Procedure Guide in full;
- You ensure all staff in your Business, responsible for accepting Card payments, read and follow the procedures detailed within; and
- You adhere to the instructions contained in this document.

You may also be asked to refer to the following, from time to time:

- the procedures outlined in the Terminal User Guide (provided with your Terminal);
- the Terms and Conditions, which are available for download on www.aibms.co.uk;
- any specific instructions or procedures relating to your facility, issued to you by AIB Merchant Services; or
- any prompts given via your Terminal.

There are particular words and phrases that are frequently used throughout this document. Please refer to Section 17: Glossary, for full explanations.

Answers to most queries regarding Card processing can be found within this Merchant Procedure Guide. If you are still unable to find an answer to your query, please contact the Merchant Support Centre on **0871 200 1436.**

If you are in any doubt as to which services your current Agreement with us covers, please contact the Merchant Support Centre.

David Courtney
General Manager
AIB Merchant Services

1. How to contact us

If you need to speak to us for any reason, our helpdesks are open Monday – Saturday, 8am – 11pm and Sunday, 10am – 4pm. Bank holiday hours are as follows - ROI & UK bank holidays 10am - 4pm, UK only bank holidays 8am - 11pm.
When you call, please have the following information to hand, if possible;

Your Merchant ID (MID)_____

Terminal ID (TID)_____

(The TID is located on a sticker at the back of the Terminal or printed on your Terminal receipt)

Support area	Query types	Contact details
Customer Service	• Funding • Changes to bank account details and business address • General Card service enquiries • Closing your account • Adding currencies and Card Not Present (CNP) facilities • Adding additional outlets • Statement queries	**0871 200 1436** (Option 1)
Terminal Support - Ingenico / Hypercom Spire / Verifone	• Mac key resets • Non functioning Terminals • Replacement Terminals • Terminal deliveries	**0871 200 1436** (Option 2 then select the relevant terminal provider)
Terminal Support - Sagepay	• Non functioning Terminals • Replacement Terminal • Terminal deliveries	**0818 313 006**
FDGL	• Leasing enquiries • Lease changes • VAT schedules	**0871 200 1436** (Option 3)
Chargebacks	• General Chargeback queries • Chargeback defence	**0871 200 1436** (Option 1)
Complaints	• To raise a complaint • To discuss a complaint	**0871 200 1436** (Option 1)
Authipay	• Authipay technical queries	**0871 200 1436** (Option 1)
AIB Merchant Services	• Investigations • Helpdesk	**aibinvestigations@aibms.com** **aib.helpdesk@aibms.com**

2. Getting Started

Your Merchant Number

When you join AIB Merchant Services you will receive a unique Merchant Identification Number (MID), which you will need to quote whenever you contact us.

Note: Should you wish to accept both Card Present and eCommerce transactions, you will need to apply (on 2 separate application forms) for 2 separate MIDs.

Point of sale display material

Before you begin to accept Card payments you should ensure that your customers are aware that they can use Credit and Debit Cards at your business. You will be given your Point of Sale material with your Terminal pack.

Using Card symbols in sales material

You can also use Card symbols and logos in your own marketing material and websites. If you'd like to do this, please go to the Merchant Support Area of www.aibms.co.uk where you can download the brand guidelines and artwork from the relevant schemes.

The Card Scheme names – MasterCard, Visa and UnionPay etc – and their associated symbols and logos are registered trademarks. As one of our customers, you are allowed to use their symbols and logos in your advertising, as long as you follow their guidelines. If you want to use American Express and Diners Club logos, you must ask these companies directly for permission.

Using Third Party Service Providers

It is mandatory that you only use registered 3rd parties (i.e. agents that have been approved by the Card Schemes) for the provision of payment services e.g. Internet Payment Gateways, Shopping Cart providers, Web Hosting services, Transaction Booking services, Back-Office for till processors etc. For more information on this, contact us.

Card Transactions explained

Card Present Transactions (over the counter)

These are Transactions where the Card and Cardholder are physically present with you at the time of the Transaction. These Transactions are conducted through Chip & PIN, Magnetic Stripe, 6 digit PIN and Signature (UnionPay) to validate a sale Transaction or Magnetic Stripe & PIN through a Terminal.
In the case of Contactless payments, the Cardholder holds their Card up to a secure reader. The card works using a secure radio signal (Near-Field Communications (NFC)) and is powered when it comes into close contact with the reader, eliminating the need to check Signatures and reducing the need to request PINs.

Card Not Present (CNP) Transactions

These are Transactions where the Card and Cardholder are not physically present with you at the time of the Transaction. These Transactions can include - Mail Order and Telephone Orders (MOTO) eg. completed order forms or fax transmissions. CNP transactions are more susceptible to fraud and are taken entirely at your own risk. **Authorisation is not a guarantee of payment.** You MUST have prior agreement from AIB Merchant Services to accept CNP Transactions.

eCommerce Transactions

These Transactions are taken over the Internet. If you wish to trade over the Internet and take Card payments, you will need a separate eCommerce Agreement and MID from AIB Merchant Services. This includes mCommerce transactions i.e. Payments taken through a mobile device.

3. Acceptable Cards and checking Cards

It is important to thoroughly check the Cards handed to you to help guard against Card fraud.

It is also important that you only accept and process Cards that have been authorised by us for acceptance by you. In a face to face environment, Transactions should be undertaken in a Chip and PIN manner only, unless the Chip is not used in the EU, in which case the following security checks should occur.

In instances where the Cardholder tells you the Chip is broken, you should seek an alternative form of payment or follow your terminal's fall back procedures (except for UnionPay cards where the Chip is not supported at this time and the Cardholder will, in most cases, use Magnetic Stripe, 6 digit PIN and Signature to validate a sale Transaction).

Security checks

The Card presented must be carefully examined to determine whether it is a legitimate Card. The validation checks listed below apply to the majority of Cards (some of which you may not accept) issued by any bank or financial institution. If the Card you are given does not fit these descriptions, it is not acceptable. Failure to follow these checks may result in you being subject to a Chargeback.

1. **Chip** – Most Cards carry an embedded Chip which works together with the Cardholder's PIN or signature. If there is a Chip, check if there has been any visible attempt to remove, replace or damage it. In the case of UnionPay, the Chip is not supported at this time and Cardholders will, in most cases, use Magnetic Strip, 6 digit PIN and Signature to validate a sale Transaction.
2. **Card brand** – This typically appears on the front of the Card and can also appear on the reverse. They should be clearly reproduced with sharp colours.
3. **Embossed or printed Card number** – The number embossed on the front of the Card may be 12 – 19 digits in length dependent on the type of Card presented.

   The simplest way to check a Card is to ensure that the last 4 digits of the Card number, embossed on the front of the Card, match the last 4 digits electronically printed on the Terminal receipt.

   For MasterCard issued Cards, the Card number always begins with a "5" or "6" and for Visa issued Cards, it always begins with a "4".

   Check for "ghost images" in the embossed Card number. These will be present if the original Card number has been flattened and new numbers embossed over the top.

   The account number on the front of the Card may be printed rather than embossed and feels smooth rather than raised.

   If the Card states electronic use only, it cannot be accepted when using paper vouchers.

4. **Valid dates** – At the Point of Sale, the Card should be carefully examined for the effective "valid from" (this does not appear on all cards) and "valid to" dates, which are located on the face of the Card. The Card Transaction date must fall on or between these dates.

   Do not accept a Card prior to the effective "valid from" date (the first day of the month) or after the expiry date (up to and including the last day of the month).

5. **Cardholder's Title and Name** – If the Cardholder's title is embossed on the front of the Card (e.g. Mr., Mrs.), check that it is appropriate to the person presenting the Card. Check that there is no obvious discrepancy between the Cardholder and the Card.

6. **Contactless indicator** – The 'wave' symbol indicates that the Card can be used to make payments without swiping it or inserting it into a Terminal. Note: This applies to contactless enabled Terminals ONLY.

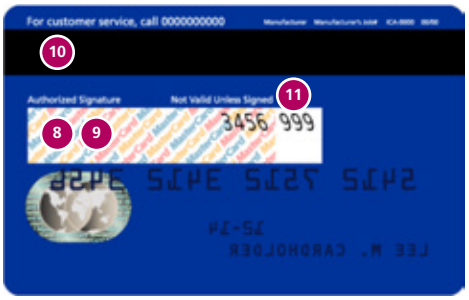
7. **Hologram** – The hologram can be on the front or back of the Card, unless a holomag tape (holographic magnetic stripe) is used in place of the traditional magnetic stripe.

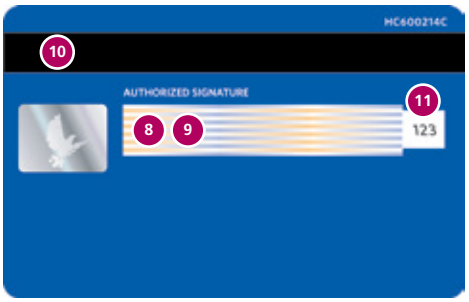
   Check that the hologram has not been tampered with. The hologram should be smooth to the touch, should not have a rough or scratched surface and the 3D image should move when tilted.

   The most common holograms are:

   - Visa – a dove in flight which moves and changes colours when tilted;
   - MasterCard – two interlocking globes which move and change colour when tilted;
   - Visa Electron – The dove hologram is optional on Visa Electron Cards;
   - Internationally issued Maestro – two interlocking globes.

8. **Cardholder's Signature** – Check the back of the Card. Make sure that the signature panel has not been disfigured or tampered with in any way (an altered signature panel may appear discoloured, glued or painted, or show eraser marks on the surface). The signature on the back of the Card must match the signature on the sales receipt (where PIN verification is not used).





9. **Unsigned Cards** – If you are presented with a Card where the signature strip (on the reverse) has not been signed, please contact the Authorisation Centre immediately for advice, stating, "This is a Code 10 Authorisation". See Section 6: Authorisation procedures. Do not allow the customer to sign the Card until you have been told what to do.

10. **Magnetic Stripe** – Ensure that the Card has a Magnetic stripe on the back, and that the Card or the stripe has not been mutilated in any way. The Magnetic stripe holds information about the Card and appears on the back of all Cards.

11. **Card Security Code** – This 3 or 4 digit security code will appear on the reverse of the Card:

    - After the last 4 digits of the Cardholder account number, if these are present or
    - On the signature panel

    For American Express Cards this number has 4 digits and is printed on the front of the Card.

Additional Security Checks

Users other than Cardholders – A Cardholder may not authorise another individual to use his/her Card for purchases. Furthermore, any Card having two signatures on the back panel is invalid.

PhotoCards – Where Cards bear a photograph of the Cardholder, ensure that the Cardholder appears to be the person depicted in the picture that appears on the Card. If you have any concerns, telephone the Authorisation Centre for advice stating, "This is a Code 10 Authorisation".

'UV' (Ultra Violet) Lamp Test – You may already use a 'UV' lamp to check for counterfeit bank notes. Cards can also be used in the same way. If you place a genuine Card under a 'UV' lamp you should see a special mark. If these features do not show, the Card is probably a counterfeit.

Code 10 - If you are worried about these or any other details, keep the Card and goods if instructed. Telephone the Authorisation Centre immediately stating, "This is a Code 10 Authorisation". See Section 6: Authorisation procedures.

Important for Visa Electron cards only

- In a Card Present environment Visa Electron Cards can only be accepted electronically, i.e. the Card must be inserted into the Chip & PIN (Personal Identification Number) reader or swiped through the Terminal and never key entered.
- Visa Electron Cards can be accepted over the Internet with full online authorisation.
- In a Card Not Present environment, key entry is permitted.
- Visa Electron Cards must not be accepted on paper vouchers under any circumstances, including under the Fallback Procedure if the Terminal is not working.

The above procedures must be adopted for all Visa Electron Card payments. If these procedures are not followed we reserve the right to Chargeback any Card Transaction.

Contactless

Contactless payment is a new way for you to accept low value Card payments for £20 or less. You key in the amount, the Cardholder holds their Card up to a secure reader and the Contactless Terminal confirms that the transaction is complete, eliminating the need to check Signatures and reducing the need to request PINs.

With payment completed in less than a second, you can serve your customers faster, cut queues and reduce lost sales.

4. Using your Terminal

The following guidelines are a brief summary of the procedures you need to follow. Full details are contained in your Terminal User Guide.

Pre Sales Check

Prior to using your Card payment Terminal fort any Transaction, please ensure the checks outlined in Section 3: Acceptable Cards & checking the Cards have been carried out and met.

Accepting Transactions – Chip & PIN Enabled Cards

Note: If the Terminal cannot read the Card or the Terminal has a malfunction, seek an alternative form of payment, follow your terminal's correct fallback procedure or refer to Section 5: Using the Paper Fallback System.

- The customer enters the Card into the Chip reader or PIN device (dependant on type of Equipment you are using, refer to procedures in your Terminal User Guide).
- All Chip and PIN Cards will prompt for a PIN code entry. Only non Chip enabled Cards will prompt for signature.
- When the above steps are complete, the customer takes their Card from the PIN device, together with any goods and a record of the Transaction.

What if the customer enters an incorrect PIN?

The customer has three chances to enter their correct PIN. If on the third attempt the PIN is entered incorrectly the PIN will lock. At this stage you should tell the customer that their PIN has locked and ask for an alternative method of payment.

IMPORTANT – If a Chip and PIN Card is presented and you process the Transaction without a PIN being entered due to a fault with your PIN pad, you WILL be liable for any Chargebacks which arise from this Transaction.

Non Chip & PIN enabled Cards and Chip & Magnetic Stripe swipe transactions

- The Cardholder enters the Card into the Chip reader or PIN device (dependant on type of Equipment you are using), or swipes the Card for Magnetic Stripe swipe Transactions. If the Terminal cannot read the Card or the Terminal has a malfunction, refer to Section 5: Using the Paper Fallback System.
- Ask the customer to sign the Terminal sales receipt and check that the signature matches that on the reverse of the Card.
- Authorisation is done automatically through your Terminal. In exceptional circumstances e.g. your Terminal has malfunctioned or is offline, you may need to undertake a manual authorisation. See Section 6: Authorisation Procedures.
- Compare the Card Number printed on the Terminal sales receipt with the last 4 digits embossed on the front of the Card. If the numbers do not match, telephone the Authorisation Centre immediately for advice, stating "This is a Code 10 Authorisation", see Section 6: Authorisation procedures.
- Once you have completed all the above steps, the Cardholder can remove the Card from the PIN device, together with any goods and receives a copy of the Terminal sales receipt.

You must retain copies of all sales receipts and refunds, securely, for a minimum of 18 months (refer to the section on PCI DSS for more information). This will assist you in checking your Merchant Statements and resolving any possible retrieval requests or Chargebacks.

Note: Any fee to be charged, and is included within the total transaction value, must be disclosed to the Cardholder prior to completing the transaction.

To prevent delays in processing Transactions, you must ensure that at the end of each business day, a banking report is undertaken on your Terminal. Please refer to your Terminal User Guide for reporting procedures.

Gratuities (Tips)

The Card Transaction amount may be changed in order to add a gratuity, in a Chip and PIN environment only, if:

- You have been authorised by AIB Merchant Services to do so;
- Your Terminal provides this function; and
- The Cardholder has given permission.

In all other cases where the Card Transaction amount has changed the Card Transaction should be cancelled. Refer to Cancelling a Card Transaction later in this section.

Deposit payments

In a delayed delivery Transaction where goods or services are to be provided at a later date and the Cardholder provides a deposit towards the full Transaction amount, two separate Card Transactions must be completed. The first is for the deposit total and second for the balance amount, which should only be submitted for payment upon delivery of the goods or provision of the services.

Note: you may only accept deposit payments or make Card Transactions using Cards which involve delayed delivery (Deferred Supply Transactions) if you have been authorised by AIB Merchant Services to do so. See Section 10: Additional Facilities.

Authorisation

Authorisation must be obtained in accordance with your Terminal User Guide and your Merchant Agreement. See Section 6: Authorisation Procedures.

Authorisation is done automatically through your Terminal. In exceptional circumstances e.g. Your Terminal has malfunctioned or is offline, you may need to undertake a manual Authorisation.

You may carry out a manual Authorisation in the following circumstances:

- Your Terminal indicates that it is necessary to do so. Please make an Authorisation call and advise the Authorisation Centre that you are calling as a result of a Terminal referral;
- You are using the Paper Fallback System, see Section 5: Using the Paper Fallback System;
- You are required to make a 'Code 10' Authorisation call. See Section 6: Authorisation procedures;
- There is a Split Sale; or
- The Card Transaction amount changes, the Card Transaction is cancelled or subsequently refunded, and Authorisation has already been obtained.

Cancelling a Card Transaction

If a Card Transaction has been processed in error or the Card Transaction amount changes you must, wherever possible, cancel the Card Transaction.

- Cancel the Card Transaction, refer to the procedures in your Terminal User Guide for more information.
- Give the Cardholder a copy of the cancelled sales receipt.
- If Authorisation was obtained for the original Card Transaction, you must telephone the Authorisation Centre. Failure to do this may result in inconvenience and embarrassment to your customer at a later date (due to the fact that funds will be incorrectly held).

Refunds

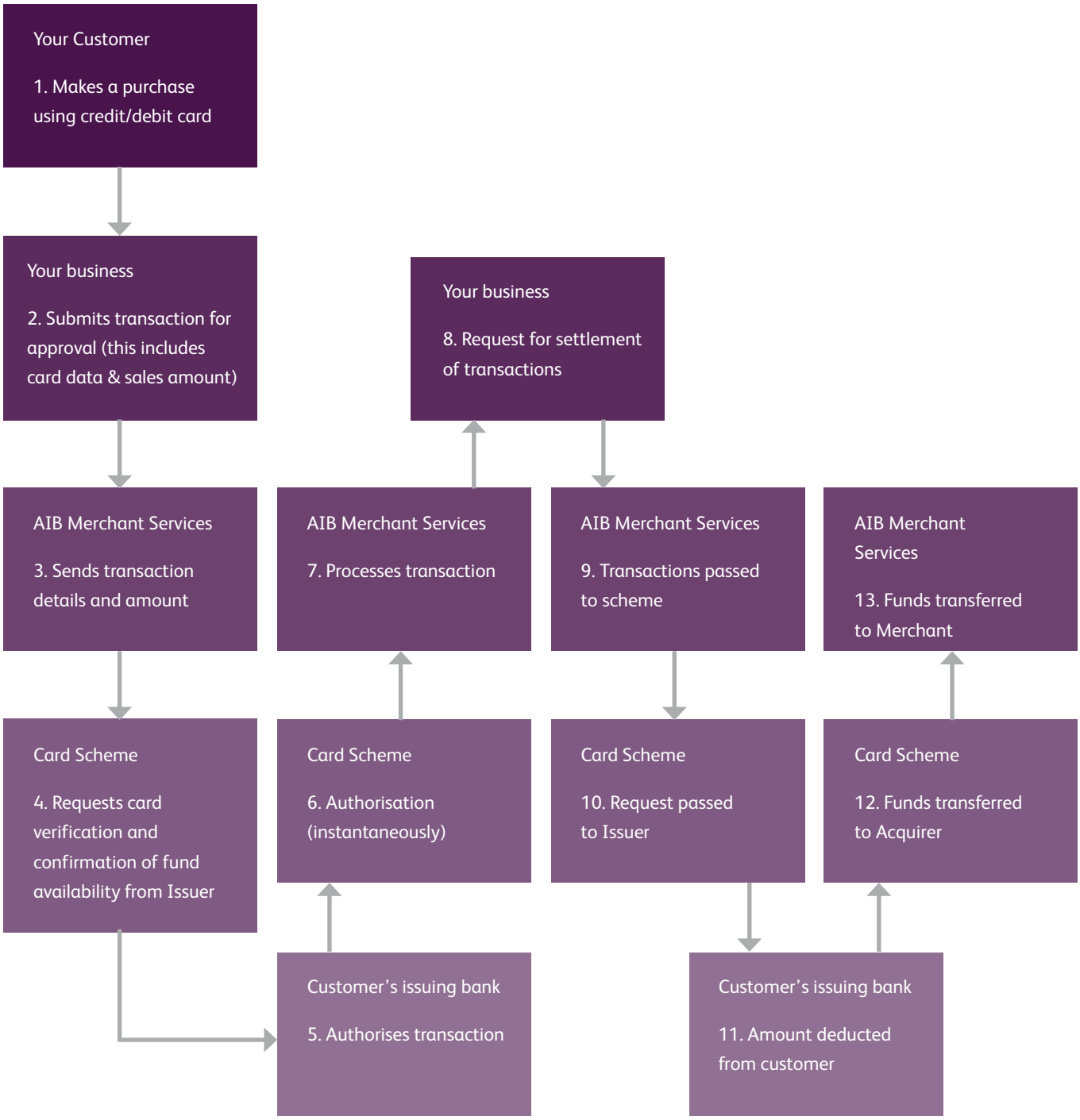
- If you wish to provide a Refund, the Refund Card Transaction must be completed using the same Card as that used for the original sale.
- You should never make a Refund to a Card where the original sale was made by cash or cheque.
- You should never make a Refund to a Card where there has been no sale Transaction.
- You should never make a Refund by cash or cheque where the original sale was made by Card.
- You must enter the Card into the Chip Card reader, PIN device or swipe it. If your Terminal is unable to read the Card you will need to manually key the Transaction into the Terminal. (Refer to your Terminal User Guide or contact us for more information)
- Where the original Transaction was PIN verified, you may need the Cardholder to enter their PIN in order to process the Refund, this will depend on the type of Terminal you use (refer to your Terminal User Guide). Otherwise you should sign the Terminal sales receipt, and make a note of the exchange and/or return of any items.
- If Authorisation was obtained for the original Card Transaction, or your Terminal indicates that a manual Authorisation is required, you must telephone the Authorisation Centre.
- You may only perform a Refund, agreed on the telephone, or in correspondence, if you are able to manually key enter Card Transactions. Please refer to the manual key entry procedures in your Terminal User Guide.
- You are not permitted to complete a Refund on your own Card and this also applies to members of your staff.
- You may only make Refunds onto Cards where authorised, i.e. goods returned, service not provided, etc.
- You are not allowed to put money into your own, your spouse's or any of your staff member's bank accounts by processing a Refund onto the relevant Cards.
- You cannot process a Refund as a form of returning winnings to a Cardholder unless specifically authorised to do so by AIB Merchant Services.

Failure to observe the procedures in this section could lead to your funds being withheld pending further investigation.

Processing and Settlement

All Transactions taken by your Card payment Terminal, must be submitted to AIB Merchant Services for processing, following which relevant funds will be lodged to your Business' bank account – this process is known as settlement.

Depending on your Terminal type, your Transactions may be automatically sent to AIB Merchant Services for processing or you may be required to manually submit your Transactions for processing at the end of the Business Day. Please refer to the Terminal User Guide that came with your Terminal to identify whether your Terminal manually or automatically submits your Transactions for processing.



There are some key points to remember:

- AIB Merchant Services have 2 processing windows, midnight and 2am. Your processing window will be dictated by the Terminal type you have. Transactions taken after 2am are included in the following day's processing cycle.
- Settlement into your bank account occurs Monday through Friday excluding Bank holidays in the jurisdiction where the receiving bank account is held.

Note: Authorisation is not a guarantee of payment.

5. Using the paper fallback system

If for any reason your Card payment Terminal is inoperable, you have the option to follow the Fallback Procedures detailed below.

If the Card is either an internationally issued or domestic Maestro Card, UnionPay Card or Visa Electron Card and repeated attempts to read the Card fail, then:

- You will not be able to manually key enter the Card details; and
- You will not be able to process the Transaction using Paper Sales Vouchers.

As you will be unable to proceed with the Transaction, you will need to request an alternate method of payment from the Cardholder i.e. another Card, or payment by cash or cheque.

If you accept internationally issued Maestro, UnionPay or Visa Electron Cards in these circumstances, you should be aware that you become liable for any Transaction which is subsequently charged back to you at a later date.

BE AWARE: In paper fallback scenarios, **do not accept prepaid cards,** and it is **not recommended to accept debit cards.**

You should contact your Terminal supplier helpdesk immediately to report any faults. A representative will endeavour to resolve the issue remotely, or failing this, will arrange for a new Terminal to be sent to your premises in the shortest time possible.

Over the counter Transactions

A Transaction can be completed by using the AIB Merchant Services Sales Vouchers that came with your Terminal. If you cannot locate these vouchers, please contact the Merchant Support Centre on 0871 200 1436 to email a template Sales Voucher to you. You can also download these vouchers on the Merchant Support Area of www.aibms.co.uk.

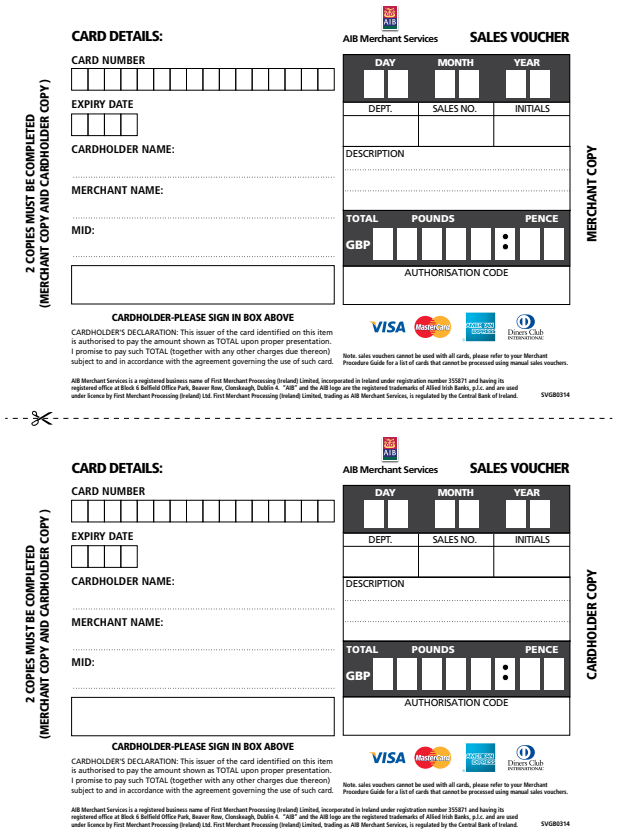
The sales voucher contains the following:

A Merchant copy: A copy of the Card Transaction must be produced to the bank, should it be requested, therefore copies must be kept securely for at least 18 months from the date of the Card Transaction. For a Recurring Transaction, copies must be kept securely for at least 18 months from the date of the last Card Transaction forming part of the recurring Transaction. If you are unable to produce a copy of the Card Transaction within the requested timescale, then the item may be subject to a Chargeback.

A Cardholder Copy: A record of the Card Transaction is to be given to the Cardholder.

Note: If you are using a Sales Voucher emailed to you by the AIB Merchant Services Merchant Support Centre or one downloaded from www.aibms.co.uk, you will have to complete both the top and bottom sections. The top section you keep for your own records i.e. Merchant Copy, and the bottom section that should be given to the Cardholder as a record of the transaction i.e. Cardholder copy.

The Cardholder MUST sign both copies.



Completing a Sales Voucher

1. Place the Sales Voucher on a firm surface.
2. Using a ballpoint pen carefully and clearly write:
    - The Card number across the top left hand of the voucher.
    - The Card expiry date directly beneath the Card number.
    - The Cardholder's name directly beneath the expiry date.
    - The Merchant name used by you and your MID.
    - Date of Transaction.
    - Amount of Transaction.
    - Give brief details of the goods purchased.
3. Where the Sales Voucher contains a carbon copy, do not mark copies with pencil or paper clips, as these can transfer through the carbons and obscure details. This does not apply when emailed or downloaded vouchers are used.
4. Please ensure that all details are clear on the Sales Voucher. If the detail is not clear, a Chargeback may occur. If you make a mistake please complete a new Sales Voucher and destroy the old one.
5. Retain the Card and check the Card details carefully. Ask the Cardholder to sign the Sales Voucher in both places.
6. When the Sales Voucher is signed check that the signature is compatible with that on the Card. Failure to do so may result in a Chargeback.
7. You must telephone the Authorisation Centre for an Authorisation Code for each Card Transaction where the Card details are handwritten. If the operator authorises the Card Transaction, write the code in the space provided on the Sales Voucher.
8. You may also wish to alert the Authorisation Centre by making a 'Code 10' Authorisation call, see Section 6: Authorisation Procedures if you suspect something is wrong e.g.
    - The Card appears unusual or has been tampered with;
    - The customer is acting suspiciously; or
    - The amount of the Card Transaction is significantly above normal for your type of business.
9. When you are satisfied that everything is in order, hand the Cardholder the bottom copy of the Sales Voucher (when using a voucher with a carbon copy) and their Card. If an emailed or downloaded voucher has been used, ensure the Cardholder has signed both sections and give one copy to the Cardholder with their Card.
10. Once the Cardholder has signed the Sales Voucher and left the Point of Sale, do not alter the Sales Voucher in any way. If there are subsequent queries or disputes, the Cardholder's copy will normally be treated as correct.
11. The Sales Voucher must always be completed in your domestic currency unless you have made arrangements with AIB Merchant Services to accept different currencies.

Once Terminal usage is available, manually enter the Transactions as per the instructions in your Terminal User Guide. If you are unsure how to do this, please contact the Merchant Support Centre.

Processing Refunds using the paper fallback system

Refund vouchers should be completed with all details in the same way as Sales Vouchers. You should then sign the completed Refund voucher. Make a brief note on the Refund voucher regarding the exchange and/or return of any items.

If goods are returned by a Cardholder and exchanged for goods of the same price, no action is required.

Never accept money from a customer in connection with processing a Refund to the Cardholder's Account.

Completing a Refund Voucher

A Refund must only be applied to the same Card that was used for the original Transaction.

If you wish to complete a Refund using the paper fallback system, you must follow the steps below:

1. Place the Refund voucher on a firm surface.
2. Using a ballpoint pen carefully and clearly write:
    - The Card number across the top left hand of the voucher.
    - The Card start date and expiry data directly beneath the Card number.
    - The Cardholder's name directly beneath the start date and expiry date.
    - Give brief details of the goods purchased.
    - Your Merchant number.
    - Your business name.
    - Your business address.
    - Date of Refund.
    - Amount of Refund.
    - Date of original purchase.
3. You must telephone the Authorisation Centre for an Authorisation Code for each Refund Transaction where the Card details are handwritten. If the operator authorises the Refund Transaction, write the code on the Refund voucher.
4. You must sign the Refund voucher.
5. Once you have completed all the above steps, return the Card to the Cardholder together with any original receipt and a signed copy of the Refund voucher.

If the cost of a replacement item differs from the returned item, a Refund for the original item should be completed on the same Card as the original Card Transaction. A new sale should be completed for the new Card Transaction and Authorisation obtained.

If a Refund is agreed on the telephone or in correspondence with the Cardholder, you should complete the Refund voucher in the manner above. You must write CARD NOT PRESENT REFUND or CNP REFUND in the signature box.

6. Authorisation procedures

When to obtain authorisation

Authorisation must be obtained at the time of the sale whilst the Cardholder is present:

- If you have an electronic Terminal, this will in most cases, obtain Authorisation for Card Transactions. However, it is your responsibility to ensure that all the relevant security checks included in Section 3: Acceptable Cards & checking the Cards, are carried out.
- The telephone number for all manual Authorisations is 0845 604 1625.

Obtain manual Authorisation if:

- The Card Transaction amount changes, the Card Transaction is cancelled or subsequently refunded, and Authorisation has already been obtained.
- You are suspicious of a Card and/or customer – in these circumstances a 'Code 10' Authorisation call should be made, see below for more information.

Authorisation only guarantees that at the Point of Sale the Card has not been reported lost or stolen and that sufficient funds are available. If you are in any doubt or are suspicious, request an alternate method of payment or complete additional checks.

How to obtain Authorisation

Take the Card and completed Voucher, (if using the Fallback Procedure) to the telephone ensuring that the goods are out of the customer's reach.

You will be required to give the following information to the operator:

- The Cardholder number.
- The Card issue number (if applicable).
- Your AIB Merchant Services MID.
- The exact amount of the Card Transaction.
- The Card expiry date.

You may also be asked for:

- The name embossed on the Card.
- If the presenter of the Card is male or female.

If requested to do so, allow the Authorisation operator to speak directly to the customer. Ensure you confirm the conversation with the operator and obtain the Authorisation code direct from the operator, not the Cardholder, before replacing the receiver. The operator may also ask you to check some additional form of identification, for example a driving licence.

Never accept an Authorisation code from the Cardholder. Please ensure that you obtain the Authorisation code from the operator directly.

If the sale is confirmed:

When the Card Transaction is confirmed you will be given a code to enter in your Terminal, see your Terminal User Guide for more information.

If the sale is declined:

No reason will be given. Please return the Card to the Cardholder, discreetly explaining that the Card Issuer has declined the Card Transaction and ask for another method of payment.

Occasionally the operator may ask you to obtain further identification from the customer or ask to speak with the customer directly. If this happens, please ensure that the telephone handset is passed back to you to speak with the operator before terminating the call.

The operator may ask you to keep the Card. Again this should be done as politely as possible and only if you feel you face no physical risk. After the customer has left, please destroy the card.

Authorisation adjustments

If there is any change in the authorised amount of the sale, or if the sale is cancelled or a refund issued, please contact the Authorisation Centre stating you wish to cancel or amend an Authorisation.

You will be asked to give:

- The Card number.
- The Card issue number (if applicable).
- The Card expiry date.
- Your AIB Merchant Services Merchant number.
- The Authorisation code quoted.
- The previously authorised amount.
- The exact new amount for Authorisation.

Recovering a stolen Card

After recovering a Card you should destroy it.

'Code 10' Authorisation applies in the following circumstances:

- The Card Number embossed on the front of the Card is different from the one printed on the signature strip on the back of the Card.
- The title on the Card does not match the customer.
- The signed name is not the same as that embossed on the front of the Card.
- The word 'void' is visible on the signature strip or there is any indication that the strip has been tampered with.
- There has been an attempt to disguise or amend the signature.
- The Card is unsigned.
- The hologram is damaged or missing.
- The Card has been mutilated.
- You have a reason to be suspicious about the sale, the Card or the customer.
- The amount of the Card Transaction is significantly higher than normal for your Business.
- Code 10' Authorisation also applies if your Terminal requests that you telephone the Authorisation Centre or the Cardholder's signature differs from that on the Card. Hold on to the Card and goods then telephone the Authorisation Centre immediately – if it is safe to do so.

You must not use 'Code 10's' to validate Cardholder addresses. Code 10 calls are not made for CNP Transactions.

7. Settlement and reconciliation

Settlement

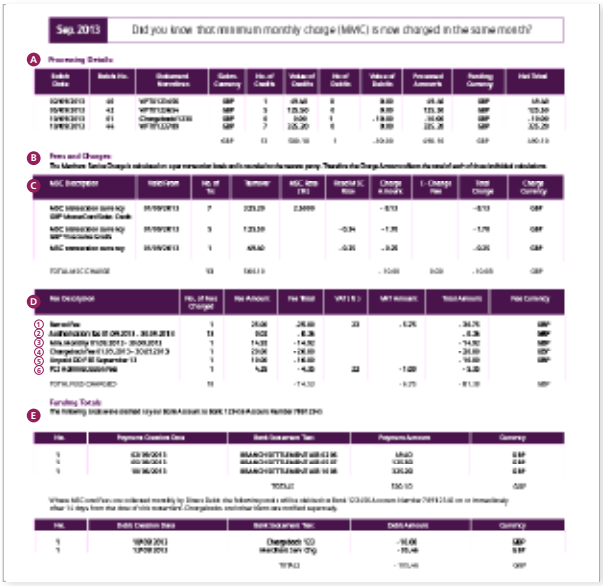
AIB Merchant Services have 2 processing windows each Business Day, midnight and 2am. Your processing window will be dictated by the Terminal type you have. Payment will be net of any suspended or rejected Transactions, which may be invalid based on Card Scheme Rules and may need to be resubmitted for processing. If you have any queries about the amount you have been funded, please contact our Merchant Support Centre and we can address these for you.

Statements

Your AIB Merchant Services Statement is issued monthly. It will explain the status of your account, including details of your monthly Transactions and other charges that may be applicable. We have included a Statement guide below to help you read and understand your Statement. There is also a more detailed guide on the Merchant Support Area of www.aibms.co.uk.

If you have additional queries, please contact us and we will be happy to help you with your query. If you would like to receive your Statement online, why not sign up to AIBMS insight (for more information, see the next page), our online data management system that offers you fast and easy access to your Credit and Debit Card Transaction data. Call us or register online at www.aibmsinsight.com.

The AIB Merchant Services Statement Guide



NOTE: This is a statement example with sample data.

A Processing Details
This area details the breakdown of all of the processing that has been funded / charged within the statement billing period (the billing period is typically from the 1st of the month to the 31st of the month). This detail is at a batch level and includes a summary of all the transactions processed in each batch.The totals of this processing will equal the total amount funded in the funding section below (see section E). So if you submit one batch per day and are setup to receive one payment per day, there will be 1 payment for each batch received and processed in the funding details at the end of your statement.

B Fees & Charges
This area of the statement includes the Merchant Service Charges (MSC) which is the cost associated with each transaction processed and the Merchant Fees, which includes any additional non processing fees. The totals of the MSC and Fees can be seen in the funding section under amounts debited, usually with a narrative of Merchant Service Charge and are collected as a single amount.

C MSC (Merchant Service Charge)
The MSC Description includes a detailed description of the card brand (VISA / MasterCard), currency (EUR, GBP, etc), type (Debit, Credit or Commercial) and any other qualification criteria, for example "Keyed Entry". The fees are grouped at the level at which they are charged so all VISA debit consumer sales will be shown as a single line.
The MSC rate and Fixed MSC rate refers to the pricing being charged for the transactions where the MSC Rate is a % of the value of the transaction and the Fixed MSC rate is an agreed per click rate per transaction. The total charged will be the MSC Rate* the Turnover or the Fixed MSC Rate* the No. of TRX, or a combination of both if both fee rates apply.

D Fees
The Fee description includes a detailed description of the Fee being charged, that may include the following:

1. **Terminal Rental Fee** The agreed monthly charge for any terminals provided by AIB (GB) Merchant Services.
2. **Authorisation Fee** An agreed fee for each authorisation request (Approved and Declined).
3. **Minimum Monthly Fee** - This is an agreed minimum monthly charge (MMC), usually £25.00 so if the MSC charge for a month is less than the MMC amount the difference between the total MSC charge (section C) and the MMC amount will be charged. In the example above, total MSC is £10.08, so the MMC is £14.92, totalling a minimum monthly charge of £25.00 (£10.08 + £14.92 = £25.00).
4. **Chargeback Fee** - This is the agreed per item administration charge for any chargeback received in the period.
5. **Unpaid DD Fee** - Fixed charge for any direct debit returned unpaid.
6. **PCI Fee** The agreed monthly compliance fee for PCI DSS (Payment Card Industry Data Security Standards).

E Funding Totals
The funding totals area of the statement gives the details of all bank transfers completed within the billing period and reconciles to the Processing and Fees and Charges totals above on the statement. This area is split into two. Amounts Credited (Funded) and amounts Debited (Charged) to and from your account(s). This area also shows the corresponding narrative that will appear on your bank statement for each item for ease of reconciliation.

Note: Go to the Merchant area of www.aibms.co.uk to access your Merchant Procedure Guide, Terms & Conditions and Terminal Quick Reference Guides etc.

AIBMS insight

AIBMS insight is an online reporting system that offers you fast and easy access to your Credit and Debit Card Transaction and settlement data.

Alongside rapid access to your data, AIBMS insight provides you with functionality to analyse, extract and archive reports, and to interrogate your data including Authorisations and Chargebacks from the past 180 days over the Internet.

You will have 24x7 access, meaning you can review your own business reports at a time that suits you. It allows group accounts (multiple MIDs) to run queries and reports across multiple entities.

Key featutres

Statements and reports

- View Statements in different formats to suit your business needs.
- Download documents in multiple formats including html, xls, pdf, zip, so you can import, manipulate and analyse data to support improved business decision-making.
- Manage and archive Statements electronically from the last six months, removing the need for manual cross-referencing, physical storage and security provision.

Search

- Quickly search and view Authorisations, Transactions, Merchant Service Charge (MSC), balances, payments, Settlements and Chargebacks.
- Track whole Transactions detailing when and how a specific Transaction was paid, including the identification of multiple Transactions in single payments.
- Search by specific date if required.
- Export data into Excel or CSV for further manipulation and analysis.

Technical specifications

AIBMS insight is a web based application requiring no installation and it is compliant with relevant PCI Security Standards.

See www.aibmsinsight.com for more information or email us at sales@aibms.com to sign up to AIBMS insight.

8. How to guard against fraud

Over the counter Transactions

Please ensure all staff accepting payment by Cards on your behalf have read and understood the following guidelines which aim to reduce the possibility of fraud and potential Chargebacks.

Please remember that Authorisation is not a guarantee of payment. If a sale appears too good to be true, it probably is.

Note: Gift card and Traveller cheque sales should also undergo the relevant fraud checks listed below.

Chip & PIN

- Chip & PIN is the most secure type of Transaction. Merchants are not required to make visual checks of the Card in Chip & PIN situations, as the Cardholder will retain control of the Card during the Transaction. Follow the prompts on your Terminal at all times.
- Be on guard if a Chip and PIN Card is presented but the PIN is blocked or the incorrect PIN is entered. You should check that this is the genuine Cardholder as you may be at risk if you accept a signature in these circumstances.
- Take care that the customer does not interfere with the Terminal or PIN pad.

Non Chip & PIN

Check the Card – If you are presented with a Card that does not have Chip and PIN, be extra vigilant.

- Do not key a Card number into your Terminal for a Transaction where the Card and Cardholder are present, this will leave you open to risk of a Chargeback.
- Use a Ultra Violet (UV) light to check the Card as most genuine Cards have special features on them that show up under a UV light – see Section 3 for more information.
- Check whether the number printed on the Terminal sales receipt is the same as that embossed on the front of the Card. This is essential for identifying a counterfeit Card. Most cases of counterfeit fraud involve 'skimming' or 'cloning'. This is where the genuine data in the magnetic stripe on one Card is copied onto another Card without the legitimate Cardholder's knowledge. Often the fraudster will not take the time to re-emboss the Card number on the Card to match the numbers in the magnetic stripe so the fraud can be easily identified with this check.
- Compare the name on the Card with the signature and the signed Voucher.
- Check whether the signature strip on the Card appears tampered with, raised or if the original signature appears to have been covered over.
- Check whether the Cardholder is taking an unusual amount of time to sign the voucher.

In any of these circumstances telephone the Authorisation Centre and state code 10.

Check the Customer

- Does the Cardholder appear nervous/agitated/hurried or are they trying to distract you by being rude or overly friendly?
- Are they making indiscriminate purchases, for example not particularly interested in the price of the item or making hasty bulk purchases?
- Are they making small item purchases with maximum value Cashback? (please ensure you have AIB Merchant Services agreement before processing any Cashback Transactions)
- Does the title of the Card match the gender of the person presenting it e.g. is a male using a Card where the title is "Mrs"?

- Be wary if the customer tells you that they are having problems with their Card where multiple Card Transactions are subsequently declined but eventually authorised for a lower value. Most genuine Cardholders are aware of the Credit that is available on their Cards.
- A fraudster may present more than 1 Card, often to find a Card that will be successfully authorised. If this happens, complete additional checks to validate the Transactions. Check that the names on the Cards presented are the same.
- Under no circumstances should a Card sale be split between two or more vouchers for the same Card to avoid Authorisation as these may be subject to a Chargeback.

Check the Transaction – is it in line with your usual business?

- Is the purchase/order substantially greater than your usual sale, for example your average Transaction value is £50 but this Transaction is £500?
- Has the Customer repeatedly returned to make additional orders in a short period of time, possibly over several days causing an unusual/sudden increase in the number and value of sales Transactions?

Remember: if the appearance of the Card being presented or the behaviour of the person presenting the Card raises suspicion, you must immediately telephone the Authorisation Centre and state "this is a code 10 authorisation". Answer all of the operator's questions and follow their instructions.

Split sales with cash, cheque or second Credit Card

If the total sale is equal to or exceeds your Ceiling Limit and payment is offered partly by MasterCard, Visa or Internationally issued Maestro and partly by cheque, cash or any other method, Authorisation must be obtained for any part of the Card Transaction being paid with by Card – even when the Card amount is below your Ceiling Limit. The Authorisation Centre should be informed that the request for Authorisation is in respect of a split sale. They may require further details.

Note: If a Transaction is above your Ceiling Limit, you should contact the Merchant Support Centre to request an increase in your Ceiling Limit and not accept split payments.

Under no circumstances should a Card sale be split between two or more vouchers for the same Card to avoid Authorisation as these Card Transactions may be subject to a Chargeback.

Additionally if a customer presents more than one Card for payment please take care and complete additional checks to validate the Transaction.

Fraud alert: In a paper fallback scenario, do not accept prepaid cards and it is also not recommended to accept debit cards.

If you have any questions or require guidance in relation to Authorisation issues, please contact the Merchant Support Centre on 0871 200 1436, then select option 1.

For security reasons your Ceiling Limit should never be displayed to the general public.

Card Not Present (CNP) Fraud, including eCommerce

Please ensure you have agreement from AIB Merchant Services before making any CNP or eCommerce Transactions. You will also need a separate MID for eCommerce Transactions.

Accepting Cards has always carried a risk and especially so when ordering goods by telephone, mail order or electronically such as over the internet. CNP Transactions, including eCommerce Transactions provide more opportunity for fraudsters, as the Card cannot be present at the time of the purchase. Businesses that are affected by CNP and eCommerce fraud can experience costly Chargebacks as well as a loss of goods or services provided.

Important

Under no circumstances can goods purchased by telephone, mail order or over the Internet be handed over the counter or collected by the customer. You will be liable for a Chargeback if the Transaction is disputed at a later date.

If a customer wishes to collect the goods then they must attend your premises in person and produce the Card. Destroy any Sales Voucher that may have been prepared and process an over the counter Transaction. If you have already processed a CNP or eCommerce Transaction you must either cancel it or perform a Refund.

There are a number of additional checks you can make to help ensure that you are dealing with the genuine Cardholder including;

- Pre-registration – before allowing your customer to purchase goods or services online, you can request that they first register as a user. You can then ask for a variety of data to establish a customer profile. Firstly verify the name and address details before deciding to accept or decline the user. You will need them to agree to your use of their personal data, as set out in your website's privacy policy. You must also ensure that their personal data is being processed fairly and legally and in compliance with the Card Scheme Rules.
- For business customers not known to you, you could check their details in the local business directory or Internet search/map engine.
- Address Verification Service (AVS) is an extra security measure that could substantially reduce the number of disputed transactions you have to deal with. AVS verifies a cardholder's billing address. The system works by checking the street address and postcode supplied by the buyer, which are included in the message you send during the normal course of a transaction authorisation.
- Independently obtain a telephone number for the Cardholder's address and telephone the Cardholder on that number to confirm the order (not necessarily straight away). You could also consider writing to the customer before dispatching goods, if you are suspicious and unable to validate by other means.
- For Internet Transactions monitor the Internet Protocol (IP) for repeated use on a number of different Transactions.
- Apply sensible limitations to the number of Cards that customers can have registered to an account and consider limiting high risk services until a customer has been validated.
- Frequency of transaction attempts using the same or similar customer information, such as name, e-mail address or IP address.

Delivery Warning Signals

Here are some danger signals to look out for when arranging delivery of goods

- If the Cardholder's delivery address is overseas, consider if the goods or services are readily available in the Cardholder's local market?
- Goods should not be released to third parties i.e. friends of the Cardholder, taxi drivers, chauffeurs, couriers or messengers (however, third party delivery of relatively low value goods such as flowers is acceptable).
- Insist that goods should only be delivered to the address that matches the Cardholder's Card. If you do agree to send goods to a different address take extra care and always keep a written record of the delivery address with your copy of the Transaction details.
- Don't send goods to hotels or other temporary accommodation. Only send goods by registered post or a reputable courier and insist on a signed and dated delivery note.

Instruct your Couriers

- To ensure the goods are delivered to the specified address and not given to someone who 'just happens to be waiting outside'.
- To return the goods if they are unable to effect delivery to the agreed person/address.
- Not to deliver to an address that is obviously vacant.

- To obtain signed proof of delivery, preferably the Cardholder's signature.

If you have your own delivery service, you may want to consider portable Terminals; please contact the Merchant Support Centre for more information.

Other Fraud Considerations

Do not under any circumstances process Transactions for any business other than your own. Fraudsters may offer commission to process Transactions when they have not been successful in obtaining their own Credit Card facilities, or you may be asked to process Transactions on behalf of a third party while they are waiting for their own facility. If you process Transactions on behalf of any other business/person you will be liable for any Chargebacks and doing so is in breach of your Terms & Conditions and will lead to termination of your Agreement.

Your Card Transactions must not involve any Card issued in;

- Your name or your account.
- The name or account of a partner in, or director of, your Business
- The name or account of a spouse or any member of the immediate family or household of any such person detailed above

Transaction Laundering

If you are approached with a proposal to buy Card Transactions, you must contact the Merchant Support Centre on 0871 200 1436, then select option 1.

This is a form of money laundering and is contrary to the terms of your Merchant Agreement.

Phishing emails / calls

If you are contacted by somebody claiming to be a bank or an official business asking for Transaction details of Cards recently accepted for payment, please advise the Merchant Support Centre on 0871 200 1436, then select option 1.

This is a fraud tactic to obtain Card details. A bank or any other official business would not make contact in this way to request Card information.

Please take care when receiving calls or visits from 'Terminal engineers'. Fraudsters will attempt to gain access to your Terminal or may manipulate you into processing fraudulent Refunds. Please always validate these by calling our Merchant Support Centre who can advise or investigate.

Note: If you receive a call from someone claiming to be from AIB (GB) Merchant Services or an engineer asking you to manually key in card details into a Terminal, please contact our Merchant Support Centre immediately. We will never ask you to do this.

Fraud Prevention Tools

Some businesses are more prone to fraud than others. It is your responsibility to protect your business from financial loss. It is imperative that you and your staff follow the contents of the Merchant Procedure Guide carefully at all times.

- Analyse Chargebacks and fraud previously suffered. It will help to identify where your business is most at risk and how fraud can be prevented in future.
- Speak to AIB Merchant Services or your PSP (Payment Service Provider) about potential fraud screening services.
- Ensure staff are continuously educated on your risk management procedures. Your front line staff are key to identifying and reducing instances of fraud.
- If you are concerned that you may be vulnerable to fraud attack, perhaps because of your business location, products or services sold or local intelligence, please contact the Merchant Support Centre and ask to speak to the fraud department who will be happy to give guidance on best practice.

Terminal security – Protecting your POS equipment

- It is your responsibility to ensure that all staff are properly trained in how to use your Terminal(s) and the security checks associated with checking Cards presented for payment.
- Supervisor Cards should be used by staff members who are fully knowledgeable in Terminal operation.
- Supervisor Cards should be kept secure and not alongside the Terminal.
- If you have any concerns that the Terminal has been tampered with, contact Terminal support on the numbers provided.

Card Security Code (CSC/CVV2/CVC2)

The Card Security Code (CSC) is the last three or four numbers on the Signature Strip on the back of the Card. For all MasterCard and Visa Cards, the code is the 3 or 4 digit number that follows directly after the Card Number. On some Cards, only the last 4 digits of the Card Number are repeated in the signature strip, followed by the 3 or 4 digit CSC.

Address Verification Service

This service allows you to check the numerical part of the Cardholder's postcode and statement address with the Card Issuer. AVS is available on all MasterCard, Visa, Maestro and American Express Cards issued in the UK. You will need to ask the Cardholder for their address as their Card Issuer records it and input the relevant numbers shown in the examples below.

Your Terminal will prompt you to enter the numeric digits in the three stages shown below:

Response	Definition	Action to take
Data Matches/ Data Matched.	This means that both the AVS and CSC match the Card Issuer's records.	As long as you have been issued with an Authorisation code, and you are satisfied that the Transaction is genuine, unless there are other suspicious circumstances that concern you, you are likely to want to go ahead with this Transaction. Although, as with all Card Not Present Transactions, payment is not guaranteed and you bear the risk if the Transaction is disputed at a later date.
Data Non Match/ Data not Matched.	The CSC and one or both of the address details do not match with the Card Issuer's records.	This is possibly a fraudulent Transaction. It could also mean that the details have been noted incorrectly. We recommend you don't proceed unless further checks are made to verify the Cardholder and the delivery address provided.
CSC Match Only.	Only the CSC matches and either one or both of the address details do not match the Card Issuer's records.	The address must match the details recorded by the Card Issuer. It is possible that the Transaction is fraudulent. It could also mean that the Cardholder has changed address and not informed their Card Issuer, or the Card Issuer does not support AVS. This could also simply mean that the details have been noted incorrectly and should be verified again with the Cardholder.
AVS Match Only.	Both address and postcode match, or just the postcode in cases where the address has a house name rather than a number. However the CSC does not match.	This could be a fraudulent Transaction. However, the Cardholder may have provided an incorrect CSC by mistake. It could also mean that the details have been noted incorrectly. You may wish to verify the CSC again before taking any further action. Beware of repeated attempts by the Cardholder to guess the CSC.
Not Checked.	This means that neither CSC or AVS have been checked.	This may be because the Card Issuer does not support either service, or their system is down. In these circumstances you will have to make a decision based on the information you have. We recommend further checks are made before going ahead with the sale.

For more information on CSC and AVS please contact our Merchant Support Centre on AIB Merchant Services - **0871 200 1436.**

IMPORTANT: Authorisation, with or without confirmation of AVS/CSC information does not guarantee payment. If fraud subsequently occurs the Merchant is liable for the Chargeback.

PCI DSS – Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that Merchants and Service Providers adequately protect Cardholder data. It defines a standard of due care and enforcement for protecting sensitive Cardholder information. The standard applies to all entities that store, process, transmit or access Cardholder data.

These Data Security Standards are developed and managed by the Payment Card Industry Security Standards Council (PCI SSC) which is an independent body that was created by the major payment Card brands (Visa, MasterCard, American Express, Discover and JCB.) to focus on improving security throughout the Transaction process.

Compliance with the PCI standards is required of all Merchants and Service Providers that store, process or transmit Cardholder data. The requirements apply to all payment channels, including retail (bricks and mortar), mail / telephone order, and eCommerce. Specific requirements vary, and are dependent on a number of different criteria including; Cardholder data storage, processing channels, security protocols, Transaction volume etc.

If you do not comply with the security requirements of the Card Associations, your business may be at risk of compromise. At this point, not only could your business be adversely impacted by loss of critical systems, but it could also be subject to significant non-compliance fine assessments by the Card Schemes.

Benefits to you

- Protection of customer's personal data.
- Increased customer confidence through a higher level of data security.
- Increased protection against financial losses.
- Maintain customer trust and safeguard reputation.

To find out more about PCI DSS, go to the PCI Security Standards Council website www.pcisecuritystandards.org

AIBMS PCI DSS Programme

It is a requirement for all Merchants to report on their PCI DSS compliance. AIB Merchant Services have partnered with Sysnet Global Solutions to provide an online merchant portal www.aibmspcidss.com to assist you in completing this process.

The programme provides you with access to a PCI Helpdesk, staffed with experts in the field of PCI DSS, to support you in complying with your obligations.

The AIBMS PCI DSS helpdesk can be contacted on 0845 874 0159.

Data Compromise event

What is a Data Compromise event?

Data Compromise events are generally deliberate attacks on systems where Cardholder data is processed or stored. They can affect the systems of Merchants, agents and third party service providers.

All data held or transmitted is at risk of compromise. Fraudsters target weak links in the payment chains to steal sensitive authentication data (Card numbers and Card security codes) and Customer's personal information (names, addresses, phone numbers, email addresses, dates of birth etc.) for the sole purpose of committing fraud.

How would a Data Compromise event affect you?

The implications for you, if you suffer a compromise, could be detrimental to your business. The public may lose their trust and confidence in your company, due to lost Customer data, causing considerable reputational damage. You could also incur Card Scheme fines. Time will be spent with PFI's (PCI Forensic Investigators) and QSA's (Qualified Security Assessors), ensuring your business has secured all vulnerabilities and is meeting PCI DSS requirements, the cost of which can be vast.

How can you protect against a Data Compromise event?

Ensure your business meets PCI DSS requirements. Information regarding the standard can be found at www.pcisecuritystandards.org.

By being PCI compliant, you are doing your utmost to ensure your business keeps valuable Customer data out of the hands of people who could use the data in a fraudulent way. Do not store any Card or personal data unless it is a requirement of your business. If it is necessary, ensure the data is encrypted in line with PCI DSS requirements.

How do you report a suspected Data Compromise event?

If you have experienced a suspected or confirmed security breach, you must take immediate action by contacting the AIB Merchant Services Merchant Support Centre on: 0871 200 1436.

Do not touch or alter your systems in any way. AIB Merchant Services will advise you if a forensic investigation is required. Touching your systems may interfere with examinations, giving false results. The PCI forensic investigator will preserve any data found on your systems prior to carrying out their investigations.

It is mandatory that you only use registered 3rd parties (i.e. agents that have been approved by the Card Schemes) for the provision of payment services e.g. Internet Payment Gateways, Shopping Cart providers, Web Hosting services, Transaction Booking services, Back-Office for till processors etc.

3D Secure

3D Secure is the payments industry authentication standard for internet/eCommerce purchases. Visa have called their version "Verified by Visa" and MasterCard have called their equivalent initiative "MasterCard Secure Code". Collectively, these are referred to as 3D Secure.

3D Secure authentication requires the Cardholder to register their Card the first time they try to purchase goods and services from an enrolled Merchant and will then be used to authenticate any future purchase at all enrolled member Merchants. In order to register, the Cardholder must answer several questions to which only the Cardholder and Card Issuer will know the answer.

The Cardholder then selects a password and a secret phrase which will be required during each online Transaction, with 3D Secure Merchants, in order to validate the authenticity of the person using the Card. Cardholders are strongly encouraged by Card Issuers to only shop online with 3D Secure registered Merchants.

3D secure is effectively the online version of "Chip & PIN" technology and used in the same way on checkout of the online sale. If you wish to participate in 3D Secure Transactions, you can obtain a Merchant plug-in product from AIB Merchant Services or your PSP. This will support the requirements of both MasterCard (through their SecureCode product) and Visa (through their Verified by Visa product).

Note: If you are a Merchant offering 3D secure, you obtain the benefit of the liability shift for fraud (for most Card types, refer to your PSP for more details) regardless of whether the Cardholder opts to do a 3D Secure Transaction or not. This doesn't stop the Card Issuers reporting fraud however, and if your fraud levels as a Merchant are deemed to be excessive by the Card Schemes, they can place you in a Chargeback window which means you lose the benefit of that liability shift despite still being 3D secure enabled. This will remain in place either until your fraud levels decrease to a level deemed acceptable to the Card Schemes or they impose a termination right on AIB (GB) Merchant Services in relation to your Merchant account.

9. Chargebacks and retrievals

AIB Merchant Services have produced an easy to follow Chargebacks handbook. This is available to download on the Merchant Support Area of **www.aibms.co.uk** or by contacting our Merchant Support Centre.

Chargebacks

A Chargeback is the return of funds from an already cleared Transaction processed on a Credit/Debit Card to the Cardholders account. A Chargeback is initiated by your Customer's card issuing bank, either at the request of the Cardholder or when the issuing bank see the need to do so via the Card Schemes. All Merchants accepting Debit and Credit Card payments run the risk of being liable for Chargebacks.

Remember you may be liable for a Chargeback, in some circumstances, even if you obtained Authorisation for a Transaction.

In certain circumstances a Cardholder or the Card Issuer has the right to question/dispute a Transaction. Such requests can be received up to 180 days from the date of providing the service and in some circumstances, beyond 180 days. If this happens please provide as much information as possible to connect the Cardholder to the Transaction. This will assist us in defending this dispute on your behalf.

CNP and eCommerce Transactions are taken totally at your own risk. If you are suspicious or are concerned, please complete additional checks to verify the customer or request an alternative method of payment.

Common reasons for Chargebacks/reversals are:

- Fraud enquiries – Cardholder denies participating in or authorising a Transaction.
- Cardholder disputes the sale for reasons such as failure to receive goods or services.
- Cardholder disputes the sale for reasons of quality.

Note: In a Chip & PIN Transaction, the liability shifts back to the Cardholder for fraud related reason codes, if a PIN is entered.

Remember you may be liable for a Chargeback even if you obtained Authorisation for a Card Transaction. Authorisation only guarantees that at the point of sale the Card has not been reported lost or stolen and that sufficient funds are available.

Retrieval requests

A retrieval request occurs when a Cardholder's bank requests a legible reproduction of the sales draft used in a Transaction.

Common reasons for retrieval requests are:

- Point of sale errors.
- Cardholder does not recognise the Transaction and information is requested from the Merchant.

10. Additional facilities

AIB Merchant Services have a proud tradition of facilitating Card payments for our customers. We have listened carefully to our Merchants ideas and suggestions, and have invested in developing additional facilities for our valued customers.

Please see below how these products can help you improve your business:

Expand your business

- Business today is multi-channel and so your payments capability needs to be too. Using AIBMS authipay, we can quickly offer you a Virtual Terminal that will allow you to take payments quickly over the phone or from any internet-enabled PC.
- AIBMS authipay is also a fully-functioning eCommerce payments platform, which can be integrated with your website to enable internet trading for your business. Reach more customers, trade 24x7 and build new sales channels – all possibilities. AIBMS authipay can bring to you.

Earn additional income

- Dynamic Currency Conversion (DCC) and Tax Free give you the opportunity to earn additional income from your AIB Merchant Services Terminal. DCC pays you a commission on Transactions where overseas Cardholders accept DCC, without any change to the Transaction processing or settlement amount and you can earn additional revenue.
- With Tax Free, your Terminal produces VAT reclaim forms for non EU visitors and you can earn a commission for each of these tax forms sent back by tourists for processing.

Be more efficient

- AIBMS insight is an online reporting service from AIB Merchant Services. Sign-up and you will be able to securely log in and access your Statement, retrieve Transaction details, reconcile Settlements, cross-analyse by location, date, Settlement details and much more. The information is right-up-to-date and can be viewed in your web browser or downloaded to an Excel sheet. You can even control and restrict access to staff members.
- AIBMS AccountUpdater is an end-to-end payments solution that allows you to take recurring payments on Debit and Credit Cards. Your customers can set the payment instruction up using just their Card number and you can use these details to bill customers the same or variable amounts on a continuous basis. A perfect solution if you take payments regularly from your customers.

Note: This is not a definitive list. To see the full range of AIB Merchant Services products and services and for all the latest developments, go to www.aibms.co.uk.

11. Card Not Present (CNP) transactions

When we refer to Card Not Present (CNP) transactions, we mean Mail Order and Telephone Order (MOTO) transactions. eCommerce transactions are covered in Section 12.

Authorisation is not a guarantee of payment. It confirms that the Card has not been reported lost or stolen at the time of the Card Transaction and adequate funds are available. If you are in any doubt or are suspicious, request an alternate method of payment or complete additional checks. Refer to Section 3: Acceptable Cards and checking the Cards.

You may ONLY accept CNP Transactions if it has been agreed in your Merchant Services Agreement. If you are approved to take CNP Transactions, you can accept payments from the following Card types - VISA, MasterCard and in some cases UnionPay.

You may only accept CNP Transactions provided they do not exceed the agreed percentage of the total Card volume, as detailed in your original application, or as agreed in your request to have CNP capability added.

If you accept CNP transactions without our express permission, you are fully liable for any Chargebacks which may ensue.

You must not accept International Maestro Cards for CNP Transactions except where the Transactions are taken through secure Electronic Commerce means (eCommerce).

When accepting a CNP Transaction, please take extra care to ensure that it is the genuine Cardholder who placed the order. Record all details in writing of the CNP Transaction and if conducted by telephone, the time and date of the conversation. You may be asked to produce this or the Cardholder's authority for a CNP Transaction, if the CNP Transaction is disputed at a later date. If feasible you should obtain and keep a copy of the Cardholder's signature on file authorising you to process the CNP Transaction.

The following orders are all acceptable as CNP Transactions:

Mail orders: written authority from the Cardholder, bearing the Cardholder's signature in any form including:

- Completed order forms.
- Facsimile transmissions.

Telephone orders: authority from the Cardholder by telephone.

If you conduct CNP Transactions by mail, for example, advertisements in magazines, the Cardholder's signature must appear on your order form and again, you must retain the instruction for at least 18 months in case the CNP Transaction is disputed at a later date. Note. It is your responsibility to ensure you are protecting and storing the data in a PCI compliant manner. See Section 8 for more information on PCI DSS.

For all orders received by mail, telephone or fax, goods must be delivered and it is advisable to retain documentary evidence of the delivery address for 18 months.

Important: Under no circumstances can goods paid by mail or telephone be handed over the counter to, or collected by, your customer.

If a Cardholder, or someone designated by them, wishes to collect the goods, then he/she must attend your premises in person and produce his/her Card.

In addition, any Sales Voucher already prepared must be destroyed and a fresh one completed as a normal over the counter sale and if you have already completed a CNP Transaction, you must either cancel the CNP Transaction or perform a Refund. See Section 8: How to guard against fraud for more information.

Information you need to record

For all CNP Transactions you must record the following details:

- The Card Number.
- The Card expiry date.
- The Card issue number (if present).
- The Cardholder's title (if present).
- The Cardholder's name and initials as shown on the Card.
- The Cardholder's address.
- The delivery address.

You may be asked to produce this information if the Card Not Present Transaction is disputed at a later date.

As telephone orders present the greatest risk, you may also wish to record the following:

- The Cardholder's telephone number.
- The time and date of the conversation.

When delivering goods, it is recommended that you take the following precautions:

- Request to see a copy of the Card at the premises.
- Where using a courier company or similar, ensure that they are instructed to only deliver the goods to the address provided and do not hand over the goods to someone outside or hanging around the premises. The courier should ensure that they also receive a signature confirming delivery of goods at the address.

Note: It is important to remain vigilant at all times as fraudsters tend to be experts at what they do and you as a Merchant suffer the consequences in the form of Chargebacks, loss of stock and in some extreme cases, penalties for information breaches. Remember, if a sale seems too good to be true, it probably is.

Completing a Card Not Present Transaction

If you are using an electronic Terminal to process your CNP Transactions, follow the instructions in your Terminal User Guide. Once you have completed the Transaction, you must indicate CNP Transactions by writing 'CNP' on the signature line of the Terminal Sales Receipt. In some cases the Terminal may have already printed this on the Terminal Sales Receipt.

Authorisation Responses

If there are available funds and the Card has not been reported lost or stolen, one of the standard responses shown below will be received. It is your decision whether or not you wish to progress a Card Not Present Transaction.

Please remember that you remain liable should a Transaction be confirmed as invalid or fraudulent, even if data matches and an Authorisation code has been issued. The final decision on whether or not to accept a payment is still up to you, as recording a security code (for more information on Card Security Codes, see Section 8) will not protect you from a Chargeback.

Response	Definition	Action to take
Data Matches/ Data Matched	This means that the CSC matches the Card Issuer's records.	As long as you have been issued with an Authorisation code, and you are satisfied that the Transaction is genuine, unless there are other suspicious circumstances that concern you, you are likely to want to go ahead with this Transaction. Although, as with all Card Not Present Transactions, payment is not guaranteed and you bear the risk if the Transaction is disputed at a later date.
Data Non Match/Data not Matched	The CSC does not match with the Card Issuer's records.	This is possibly a fraudulent Transaction. It could also mean that the details have been noted incorrectly. We recommend you don't proceed unless further checks are made to validate the Cardholder.
Not Checked	This means that the CSC has not been checked	In this instance, you will have to make a decision based on the information you have. We recommend further checks are made before going ahead with the sale.

For more information on CSC please refer to Section 8: How to guard against fraud for more information or contact our Merchant Support Centre on 0871 200 1436.

Important: Authorisation, with or without confirmation of CSC information does not guarantee payment. If fraud subsequently occurs the Merchant is liable for the Chargeback.

Authorisation

International Maestro, MasterCard and Visa Cards

Authorisation must be obtained for all sales. The Cardholder must be advised of the delivery timeframes, any special handling arrangements and of the cancellation policy. Shipping dates for goods must be within 7 days of the date Authorisation was obtained. If after the Card Not Present Transaction has been taken, additional delays occur (e.g. item becomes out of stock) the Cardholder must be notified and the Card Not Present Transaction re-authorised.

When telephoning the Authorisation Centre you will be required to clearly state in this order:

1. "This is a Card Not Present Transaction Authorisation".
2. Card Number.
3. Your AIB Merchant Services MID.
4. Exact amount of sale.
5. Card expiry date.
6. Cardholder name, initials and address, including postcode.

You will be given an Authorisation code to be written in the space provided on the Voucher or Card Not Present Transaction Schedule.

If there are unacceptable levels of fraudulent Card activity and/or Cardholder disputes resulting from Card Not Present Transactions, AIB Merchant Services reserve the right to withdraw your Card Not Present facility.

Note: It is your responsibility to ensure you adhere to PCI DSS regarding the storage and protection of customer data, see Section 8 for more information on PCI DSS.

12. eCommerce Transactions

To accept eCommerce payments, you will need an eCommerce MID (Merchant ID) from AIB Merchant Services. This is required even if you already have a Merchant account for Card Present payments. This involves a new application to AIB Merchant Services for your eCommerce facility and once this is approved, you will be issued with a new MID that must be used for all eCommerce Transactions.

Note: It is mandatory that you only use registered 3rd parties (i.e. agents that have been approved by the Card Schemes) for the provision of payment services e.g. Internet Payment Gateways, Shopping Cart providers, Web Hosting services, Transaction Booking services, Back-Office for till processors etc.

Website requirements

If you make a change to your web page content, you must submit printouts to AIB Merchant Services for review. AIB Merchant Services may terminate your ability to accept Transactions over the Internet if changes on the web pages are not submitted for approval.

Research into the use of Internet sales solutions have shown that up to half of eCommerce related disputes result from poor service from eCommerce Merchants offering Internet facilities. To reduce the risk of disputes with Cardholders, you will need to adhere to the following requirements.

Placing an order

When a Cardholder places an order through your website you must (unless the recipient is a business and you have both opted out of these requirements):

- Provide details of the different technical steps to conclude the contract and whether the contract will be kept by you and accessible to the Cardholder.
- Acknowledge receipt of the order to the Cardholder without undue delay and by electronic means.
- Make available to the Cardholder appropriate, effective and accessible, technical means allowing the Cardholder to identify and correct errors prior to placing an order.
- Provide information in relation to any relevant codes of conduct to which you subscribe and how these can be consulted; and
- Make available to the Cardholder any applicable Terms and Conditions in a way that allows the Cardholder to store and reproduce them.

Payments and Refunds

- You MUST ONLY Credit refunds to the same Cardholder Number that was used in the original payment, you can NEVER Credit another Card number. Failure to comply may lead to a Chargeback.
- The Cardholder should be provided with clear information on all payment options and clear instruction on how to pay.
- Your website must be secure for sending personal and financial information – 128 bit key Encryption at a minimum.
- Your customer should be informed of their cancellation rights and their rights to a Refund and/or replacements at the time of purchase/and the conditions for exercising the cancellation rights.
- A refund information page should also be provided with clear contact details.
- Receipts should be provided with the goods on delivery.
- The Cardholder should be provided with details of how and to whom a complaint can be made including an address.

Receipt requirements

You must provide a Cardholder receipt and it must contain at a minimum the following information:

- Concealed Card Number: For eCommerce Transactions, the Card Number must not appear on the Transaction receipt. This is a fraud prevention requirement to ensure that Card details are not compromised;
- Unique Transaction identifier: To assist in dispute resolution between you and the Cardholder. You must assign a unique identification number to the Transaction and display it clearly on the Transaction receipt;
- Cardholder name;
- Transaction date;
- Transaction amount;
- Transaction currency;
- Authorisation Code;
- Description of Merchandise or Services;
- Merchant name; and
- Website address.

You can choose to send the Cardholder this required information in one or both of the following ways:

(a) An E-mail outlining their information, and/or

(b) A physical receipt by post.

To minimise Cardholder enquiries, you are encouraged to display an online acknowledgement of the Transaction. When this online acknowledgement is sent, we advise that you include a Statement encouraging the Cardholder to either print or save this document for their own records.

Recurring payments

AIB Merchant Services now offer an end to end solution for recurring payments, which allows eCommerce Merchants to capture payment details once, and be able to use these over time to charge fixed or variable amounts, as is agreed with the Merchant, when providing the initial Card details.

Merchants who may benefit from such a facility include;

- Utility or other Merchants with a regular billing cycle;
- Merchants who offer products or services on a subscription basis;
- Merchants who collect payments in instalments; or
- Merchants who wish to offer a service where the customer can use account details held on file for future purchases.

AIBMS AccountUpdater includes the facility to have all Visa and MasterCard details updated monthly, ensuring that payments are not disrupted by customer Cards being stolen, expired or replaced by issuers. To avail of AIBMS AccountUpdater, please contact AIB Merchant Services for further details.

Note: Recurring Transactions can only be processed with the permission of AIB Merchant Services.

Merchants must ensure that repeat Authorisation requests, following a decline, are limited to a maximum of one Authorisation request per day and such requests must cease after 31 days.

Delivery and Guarantees

- Delivery dates and times should be clearly stated and agreed with the Cardholder. If it is not possible to deliver on the agreed date and time, another delivery should be arranged. If this is not possible, the Cardholder should be offered a Refund.
- You should record both billing address and delivery address details, where these differ. To reduce the likelihood of a dispute, you must verify the address details to confirm that they are valid and registered to the customer. In the event of non-delivery, it is your responsibility to prove receipt of the goods by the Cardholder.
- Guarantee terms and details should be clearly stated. The Cardholder needs to be aware that this will, in no way, affect their statutory rights. The name and address of any third party backing the guarantee should be provided.
- Apart from deposits, full payments for goods or services must not be debited from a Cardholders Account until the goods have been dispatched or the service provided. Should you wish to be able to take deposits on goods or services, you must secure an agreement from AIB Merchant Services for this before any deposits are taken.

13. eCommerce security guidelines

We recommend using AIBMS authipay as your secure payment gateway.

Card Encryption

Sensitive Data transmitted from the web Browser (including all Card details) to any Server should be protected using a minimum of 128-bit SSL.

You may choose to have your website hosted by a PCI compliant ISP, which meets these security guidelines.

Any Card Data stored on an ISP's Server must remain in an encrypted form at all times.

You must ensure that all Transactions are processed using the minimum security Encryption standards approved by AIB Merchant Services. A Transaction must never be taken on the Internet without using approved Encryption software.

Physical Security

All communication equipment (including any Firewall technology) and Servers must reside in a physically secure area.

Access to the secure area must be controlled and restricted to authorised users only.

Network Security

Firewall technology must be in place between any employed Servers involved in Internet trading.

The Firewall technology should restrict the communication passing through the network and filter information to the minimum requirement.

A traffic-filtering element must be presented which is able to prevent "Spoofing". This will prevent unauthorised access to your Server by individuals that are not who they claim to be.

The system must be audited daily to identify any attempted or actual breaches of the integrity of the Firewall.

The system must provide user authentication (individual accountability) as required, including, when necessary, token authentication.

Internet Service Security

The Server file system must be secured to allow access to the minimum Data required to perform the service.

The Server must run the minimum number of external network services possible.

System Administration

The Internet system should authenticate the system administrators individually using regularly changed passwords.

The system should log all actions performed by the system administrators to provide an audit trail.

Auditing

An audit trail should be kept of all Internet Transactions

Back Up

All Server Data should be backed up on a regular basis. The backup should be securely stored at an offsite location.

Cardholder numbers relating to Transactions should be cleared from the Server at least every two weeks.

The Transaction details must be stored offline and securely for a minimum of 12 months from the dispatch date of goods, or provision of the services.

Under no circumstances, either on paper or on any system, should you retain Card Security Codes (CSC / CV2 / CVV2) when accepting CNP Transactions. Card Security Codes must be destroyed once the Transaction is completed. For more information on this see Section 8: How to guard against fraud.

Security System

By applying for an Internet facility with AIB Merchant Services as part of your Merchant Agreement, you confirm that you will:

1. Prevent Cardholder information or Transaction data from being disclosed intentionally or otherwise;
2. Prevent unauthorised access to systems and applications;
3. Prevent loss of Data or loss of Data integrity stored on any PC or Server; and
4. The electronic form used to process the Transaction must contain the following information:
    - Transaction amount.
    - Card type (Visa, MasterCard, UnionPay, Amex, Diners, Discover).
    - Cardholder number.
    - Card valid from date.
    - Card expiry date.
    - Cardholders full name.
    - Cardholders billing address.
    - Cardholders delivery address.

14. Complaints procedure

At AIB Merchant Services, we place great importance on providing the highest standard of service to all our customers.

If, for any reason, you are not entirely satisfied with the level of service you have experienced from us, we would like to hear from you and we will endeavour to put it right.

Who to Contact

We have internal procedures for handling complaints fairly and speedily. These include acknowledging your complaints within 24 hours and letting you know how long it might take to investigate it and respond more fully.

If you wish to make a complaint you should first of all contact our Merchant Support Centre and outline the reason and details for your complaint. All complaints are thoroughly investigated and you will be supported and updated throughout the investigation.

AIB Merchant Services
Merchant Support
PO Box 6324
Basildon SS99 9EG

0871 200 1436 Option 1

15. How to end your Merchant Services Agreement

If you wish to terminate your AIB Merchant Services Agreement, refer to the termination provision in your Terms & Conditions. If you cannot locate your copy of the Terms & Conditions, you can download a copy from the Merchant Support Area of www.aibms.co.uk or contact the Merchant Support Centre on 0871 200 1436 who will be able to advise.

Managing your Terminal when ending an Agreement

Following termination of your Merchant Services Agreement, all Terminals must be returned immediately, or you may be liable for charges associated with their non-return.

Where you have a Terminal provided by AIB Merchant Services under a rental arrangement, you must contact our Merchant Support Centre to arrange return of the Terminal.

Where you have a Terminal provided by First Data Global Leasing (FDGL), under a lease agreement, you must contact FDGL directly to discuss your termination terms otherwise you will continue to be debited following the termination of your Merchant Services Agreement. You should refer to your FDGL lease agreement for more information.

If you are unsure whether your Terminal is supplied by AIB Merchant Services, please contact our Merchant Support Centre who can advise – 0871 200 1436 and select Option 1.

16. Other useful information

Changes in your business

Changes in your business may require you to inform AIB Merchant Services. This will ensure that we are funding the correct bank account, have up to date contact details for statements, letters and deliveries and that the contacts for your business are up to date.

We MUST be informed in the following situations;

- Should you move bank accounts or employ a new staff member who is authorised to contact AIB Merchant Services to log issues or discuss your account, please call the Merchant Support Centre to advise them of the change.
- Changes to bank accounts will require a Direct Debit Mandate Change. If you need to change your bank details, please call our Merchant Support Centre who will be happy to explain the process and make the necessary changes

If you do not let us know about any of the above changes, we may suspend or withdraw some or all of your Card processing facility.

Change of Legal Entity/Change of Legal Name

Some changes in a business will cause a Change of Legal Entity or a Change of Legal Name. This takes place whenever one of the following occurs:

- The Business undergoes a change of ownership;
- New directors have joined the company;
- Directors have left the company;
- The business has changed from a Sole Trader to a Limited Company;
- The business has changed from a Limited Company to a Sole Trader; or
- The business “legal name” has changed.

It is critical that you notify AIB Merchant Services of these changes to ensure that your business is correctly funded and to prevent issues arising after the change in your business. Some changes may incur an administration fee. Please contact our Merchant Support Centre for more information.

Where a Merchant has a Card payment Terminal, leased from FDGL and undergoes a Change of Legal Entity or Change of Legal Name, you must contact FDGL and make them aware of the change.

Brand materials

MasterCard and Visa all provide brand guidelines and materials for use by Merchants. We have provided links to the brand guideline sites for you below.

From here you can simply download the brand mark for use on your website or printed collateral and access brand guidelines to show you how to implement the logos into your own designs. See the “Card scheme brands” area on our website for more information.

Diners/Discover brand suite

To go to the Diners/Discover brand suite link access http://www.discovernetwork.com/merchants/signage-logos/index.html

MasterCard brand suite

To go to the MasterCard brand guidelines link access www.mastercardbrandcenter.com

Visa brand suite

To go to the Visa brand suite link access http://corporate.visa.com/newsroom/visa-logos-and-images.shtml

Card schemes

Below you will find additional information on Card schemes for MasterCard, Visa, UnionPay, Maestro and American Express.

American Express
www.americanexpress.co.uk

Diners/Discover
www.discovernetwork.com

Maestro
www.Maestrocard.com

MasterCard
www.mastercardmerchant.com

Union Pay
www.unionpay.com

Visa
www.visaeurope.com

Useful websites

For Merchant services information: www.aibms.co.uk

Our compliance programme: www.aibmspcidss.com

Payment gateway facilities: www.authipay.com

For payment news: www.transactionage.com

Our online reporting system: www.aibmsinsight.com

Global leader in payment services: www.firstdata.com

For business banking: www.aib.ie/business

Irish Payment Services Organisation Limited: www.ipso.ie

SafeCard: www.safecard.ie

For advice on Card fraud prevention: www.cardwatch.org.uk

UK payments administration: www.ukpayments.org.uk

The UK Cards Association: www.theukCardsassociation.org.uk

For advice on Contactless acceptance: www.contactless.info

17. Glossary

Address Verification Service (AVS): a service that issuing banks perform during authorisation. Using this service, the billing address that customers enter when placing an order are compared to their addresses kept on record at the bank.

Agreement: Refer to your Terms and Conditions for the meaning. The Agreement sets out the Agreement understanding and undertaking of the parties in relation to the provision of the Services by AIB Merchant Services to you.

AIB: Means Allied Irish Banks plc.

AIB Merchant Services: Means AIB Merchant Services, the trading name of First Merchant Processing (Ireland) Limited, a joint venture between Allied Irish Banks plc. and First Data Corporation.

Authorisation: Means a process whereby a Transaction for a specified amount is approved or declined by a Card issuer or an Acquirer on behalf of a Card issuer. This approval confirms that the Card number is valid, that the Card has not been reported lost or stolen and that funds were available in the account at the time of the Transaction. It does not confirm the authenticity of the Card presenter or the Card, or guarantee settlement of the Transaction.

Authorisation Centre: Means the AIB Merchant Services Credit Card centre or such other centre as we may from time to time establish and notify to you.

Authorisation Code: Means a code number advised by the issuer to us when an authorisation request is approved.

Browser: Means the software used to view information on the internet. Browser software is usually provided as part of a standard software package when purchasing a new PC.

Business Day: Means any day the Bank is open for business in Great Britain.

Business: Means your Business as a Merchant as described in the Agreement or such other description as AIB Merchant Services may agree from time to time.

Card: Means all valid and current payment Cards approved by AIB Merchant Services and notified to you in writing from time to time.

Cardholder: Means an individual, company, firm or other body to whom a Credit or Debit Card has been issued and who is authorised to use that Card.

Cardholder's Account: Means an account in the name of the Cardholder, as identified in the Card Number.

Cardholder's Information: Means any information in relation to a Cardholder including any Card Number and personal data.

Card Issuer: Means the institution that issued the Card to the Cardholder.

Card Not Present (CNP): Means an order for goods or services where the Card or the Cardholder is not physically present at your premises at the time of the Transaction. This often arises from postal or telephone requests for goods or services.

Card Number: Means the number displayed on a Card identifying the Cardholder's Account.

Card Present: Means a Transaction where the Card is physically presented to you by the Cardholder as the form of payment at the time of a sale.

Cashback: Means a service provided to Cardholders whereby cash is dispensed with a Debit Card purchase transaction at the Point of Sale.

Cashback Limit: Means the maximum amount of cash that you may provide to a Cardholder as part of a Purchase with Cashback as we may notify from time to time. This is set by the Card Schemes, the maximum amount allowed by the Card Schemes is €100 but this can be lower with some Merchants.

Chargeback: Means a demand by a Card Issuer or a Card Scheme to be repaid a sum of money by us in respect of a Transaction, which

has been previously subject to Settlement and for which we have been paid by the relevant Card Scheme.

Chip: Means an electronic device in a Card, which enables the Card to communicate Cardholder details to a Chip and PIN Terminal.

CSC/CVV2/CVC2: Means the three or four digit security code printed on the reverse of Card and intended to enhance the authentication of the Card.

Data: Means Card Transaction and Refund data.

Direct Debit: An instruction given by you to your bank, to permit us to demand or initiate payment of sums due to us from the Nominated Bank Account in accordance with relevant Scheme Rules.

Electronic Commerce: Means a non-face-to-face online Transaction using electronic media in which Card details are transmitted by a Cardholder to you via the Internet, the extranet or any other public or private network.

E-mail: means Electronic mail sent from computer to computer.

Encryption: This is a method of scrambling a message so that an unauthorised third party does not easily read it. Using complex mathematical algorithms, which are then decoded using a key to unlock the Data, encrypts messages.

Equipment: Means all equipment provided to you under a Leasing agreement by AIB Merchant Services, our agents, or any other entity in the AIB Merchant Services Group, including in particular any imprinter, electronic data capture device or Sales Vouchers and including any replacements, substitutions or additions thereto.

Fallback Procedures: Means the manual procedures to be followed when the Terminal cannot connect to the processor's system. This refers to both paper vouchers and the swipe functionality (refer to Section 5).

Firewall: Means a combination of computer hardware and software that separates a connected network into two for security purposes. A Firewall filters the information that is passed between the Internet and your system.

Floor Limit: Means the amount above which authorisation is required in respect of a Transaction, as determined by the relevant Card Scheme or us from time to time.

Internet: Means the Internet being a collection of various separate networks worldwide, which are connected together, using a standardised set of communication protocols.

Internet Service Provider (ISP): Means the provider of a service to enable Card details to be sent securely over the Internet to enable payment to be made for goods or services.

Issuer: Means an organisation that issues Cards and whose name appears on the Card as the Issuer or who enters into a contractual relationship with the Cardholder for the use of the Card.

Merchant Service Charge (MSC): Means a percentage charge that AIB Merchant Services applies to you for the handling of Visa and MasterCard Transactions.

Payment Service Provider (PSP): Means a provider of a service, which enables online and offline business to take card payments securely.

PCI DSS: Means Payment Card Industry Data Security Standard (PCI DSS) which is a set of requirements designed to ensure that ALL companies that process, store or transmit Credit Card information maintain a secure environment. The PCI DSS are administered and managed by the PCI Security Standards Council, an independent body that was created by the major payment Card brands (Visa, MasterCard, American Express, Discover and JCB). Further details about the PCI DSS can be found at www.pcisecuritystandards.org

PIN (Personal Identification Number): This is the secret number used by Cardholders with Chip Cards to authorise Transactions to be debited to their account.

PIN Pad: Means a secure device with an alphanumeric keyboard, which complies with the requirements, established from time to time by us and through which the Cardholder can enter their PIN.

Point of Sale: Means the physical location at which goods are sold to customer. This is often more specific than the actual location in the case of Card Not Present Transactions, where you accept Transactions via a website or phone.

Recurring Transaction: Means a Transaction that the Cardholder has agreed can be debited to their Cardholder's Account at agreed intervals or on agreed dates. The Transaction can be for a specific amount or for an amount due to you for an ongoing service or provision of goods.

Refund: Means where you agree to make a Refund to the Cardholder's Card of the whole or part of any sum authorised by a Cardholder to be debited to their Cardholder's Account.

Refund vouchers: Mean vouchers to be used during Fallback Procedure.

Sales Vouchers: Mean vouchers to be used during Fallback Procedure.

Schemes: Means Visa International, MasterCard International, International Maestro and other schemes notified to you by AIB Merchant Services from time to time.

Scheme Rules: Means the rules and operating instructions issued by particular Schemes from time to time.

Secure: Is a minimum of 128 bit key Encryption (or as we tell you from time to time).

Secure Socket Layer (SSL): This is an Internet Protocol that enables encrypted Card payment Transactions to be made over the Internet.

Server: Means a computer that allows Internet Services and the exchange of Data.

Service Charge: Means a charge that AIB Merchant Services levies on you for the services provided to you by us.

Settlement: Means the payment of amounts to be paid by us to you or by you to us under this Agreement.

Spoofing: The creation of illegitimate websites that appear to be published by established organisations.

Statement: Means the regular advice from AIB Merchant Services to you advising of the Transactions performed by you and the charges due by you.

Terminal: Means an electronic device used to capture Card details, for obtaining authorisations and submitting Transactions to us for Settlement. The term also includes any PIN entry device (PED) if it is a separate device.

Terminal Supplier: Means any company authorised by us to supply Terminals to Merchants.

3D Secure™: Means the Three-Domain Secure protocol developed by the Card Schemes and for the Agreement includes "Verified by Visa" and "MasterCard SecureCode" and such other programmes notified to you by AIB Merchant Services from time to time.

Transaction: Means an act between the Cardholder and you regarding the purchase or return of goods or services where the Cardholder uses his Card to pay for such goods or services that results in the generation of a Transaction Record and the providing of goods or services and/or Refunds.

Transaction Data: Means all data relating to Transactions.

Transaction Record: Means the particulars of a Transaction required from you by AIB Merchant Services in order to process a Transaction in the form as prescribed by us.

You or your or Merchant: Means the Merchant who has entered into the Agreement.

AIB Merchant Services

How to get in touch

Call us 0845 301 5407

Drop a line to our team on sales@aibms.com

Click on www.aibms.co.uk

If you have any questions, just ask.

AIBMS GBMPG0514