# AIB Merchant Services - Merchant Procedure Guide

## Issue date: September 2024



**Author:** Sinead O'Rourke

**Next Review Date:** September 2025

# Contents

# 1. About AIBMS

Thank you for choosing AIB Merchant Services. We are one of Irelands largest providers of card payment services offering; online, in-store and on-the-go solutions. We are committed to delivering a first-class client experience through our performance, service and products.

This guide contains important information about the services we offer along with the procedures you as a merchant should follow when processing card payments. It is an important part of your agreement with AIBMS, as defined in the Terms and Conditions of Use, for the provision of AIBMS services.

Therefore, it is important that:

- You read this Merchant Procedure Guide in full.
- You ensure all staff in your business who have responsibility for accepting card payments have read and understood the document.
- You and your staff adhere to the instructions contained in this document.

This document is intended to go hand in hand with other important documents, such as the AIBMS Terms and Conditions, Chargeback Handling Guide and Product User Guides

# 2. Getting Started

## 2.1 Your Merchant ID (MID)

When you become an AIBMS customer, you will receive a unique Merchant Identification Number (MID). This is an important number which you will need to reference anytime you need to contact us.

Depending on how many outlets or solutions you have, you may have more than one MID, your MID can be found on your statements.

## 2.2 Support Centre

We offer several channels by which you can contact us:

### 2.2.1 Self-Service Portal

Manage your account at a time that is convenient to you via our online **self-service portal.** The portal is available via our website www.aibms.com.

### 2.2.2 Email

You can contact our support teams via the **Contact Us** page, available on www.aibms.com.

### 2.2.3 Web Chat

You can instant message our team via **WebChat**, also available via www.aibms.com.

### 2.2.4 Telephone

Or alternatively, you can speak to us on the relevant number below:

| Service Area | Queries | Contact Details |
|---|---|---|
| Customer Service (Account Support) | - General Enquiries<br>- Funding Enquires<br>- Change of Bank details<br>- Change of Address<br>- Adding additional facilities<br>- Adding additional outlets<br>- Statement queries | **ROI:** 0818 021 062<br>**NI:** 0371 200 1437<br>**GB:** 0371 200 1436<br><br>**Email:** customerservice@aibms.com |
| Technical Support | | Please refer to the sticker on your card machine |
| Authipay | - Technical queries regarding your Authipay product | **ROI:** 0818 021 062<br>**NI:** 0371 200 1437<br>**GB:** 0371 200 1436<br><br>**Email:** authipay@aibms.com |
| Chargebacks | - General chargeback queries<br>- Defending chargebacks | **ROI:** 01 247 6483<br>**GB:** 01268 298981<br><br>**Email:** chargebacks@aibms.com |
| Complaints | - Raising a complaint<br>- Discussing an open complaint | **ROI:** 0818 021 062<br>**NI:** 0371 200 1437<br>**GB:** 0371 200 1436<br><br>**Email:** aibcomplaints@aibms.com |

## 2.3 Transaction Definitions

- A **Card Present (CP)** transaction takes place where the cardholder is physically present at the time of the transaction. These transactions are captured through either chip and pin or contactless.
- A **Card Not Present** transaction (CNP) takes place where the cardholder is not physically present, such transactions typically take place over the phone. Another example of a **Card Not Present** transaction is where the cardholder is present, however their card details are manually keyed into the machine. **Note: Card Not Present transactions are more susceptible to fraud and are taken at your own risk.**
- An **eCommerce** transaction takes place over the internet. eCommerce transactions typically take place through a website, a mobile app, or using a payment link.

You must gain prior approval from AIBMS to take payments across these different channels.

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 AIBMS to do so.

## 2.4 Taking Payment

Full instructions on how to use your card machine to accept payment can be found in your Terminal User Guide.

### 2.4.1 Card Present

Generally, when you input the value of the card payment into the device, it will instruct the cardholder to insert or tap the card. Please see below the full list of acceptance methods:

***Contactless***

If the transaction falls below a certain amount (€50 / £45) the customer can tap their card against the card reader. In the event that the customer has performed more than 5 consecutive contactless payments, or where their prior contactless payments have exceeded the value of €150, the customer will be asked to insert their card and enter their PIN.

***Chip & PIN***

If the customer inserts their card, it will automatically prompt for PIN code entry. Once the transaction is authorised, the customer can remove their card from the device and a receipt will be made available to them.

***Swipe & Signature***

The vast majority of cards now carry a chip, however from time to time you may come across a card without a chip, or where the chip is damaged. In these circumstances, you may be required to swipe the card and have the cardholder sign the voucher.

*Please be advised that accepting swipe transactions constitutes an increased level of risk as the local security feature, chip and PIN, is bypassed.*

**Note: Swipe transactions are more susceptible to fraud and are taken at your own risk.**

Please familiarise yourself with the guidance laid out in section 4.1.1. This guidance is designed to help you guard your business against fraud.

### 2.4.2 Card Not Present (CNP)

Card Not Present transactions can be performed by keying the transaction manually into your card machine or by using a Virtual Terminal. Please refer to the relevant user guide for more information.

**Note: Card Not Present transactions are more susceptible to fraud and are taken at your own risk.**

You may only accept CNP transactions if you have prior approval from AIBMS to do so, and these must not exceed the agreed percentage of total card volumes, as detailed in your application for CNP capabilities to be enabled on your merchant account.

AIBMS reserves the right to withdraw Card Not Present processing facilities if it observes unacceptable levels of fraudulent card activity or high levels of chargebacks.

Please familiarise yourself with the guidance laid out in section 4.1.2. This guidance is designed to help you guard your business against fraud.

### 2.4.3 eCommerce

eCommerce transactions are those performed over the internet. You must only use 3rd party providers (such as payment gateways, merchant plug-in providers and PCI-DSS service providers etc.) that are approved by the card schemes.

AIBMS requires that all merchants engaged in eCommerce transactions to be registered with the applicable card scheme for the use of 3D Secure. 3D Secure is a security protocol developed by the card schemes and includes Verified by Visa and Mastercard SecureCode, and other such programmes that AIBMS may notify you of from time to time.

You must fully comply with the requirements of the Second Payment Services Directive (PSD2) that 3Ds v1 or v2 be used as a Secure Customer Authentication (SCA) in all applicable transactions as defined in PSD2 by the European Banking Authority.

If you are unsure as to whether the type of transactions you process require Secure Customer Authentication, you can check your transaction type in our PSD2 Health Check: https://www.aibms.com/psd2/

The application of 3D Secure protocols are primarily managed by your Payment Service Provider. It is your responsibility to enquire as to the setup that is in place with your payment gateway to ensure that Secure Customer Authentication parameters are correctly applied.

This is in the interest of protecting cardholders and merchants alike.

## 2.5 Refunds

If a transaction has been processed in error, you may void the transaction immediately after. Please refer to the relevant user guide for more information on voiding a payment (NB: not all device types can support voids).

If you need to issue a refund, please refer to the relevant user guide for instructions on how to perform a refund using your payment facility.

When issuing a refund:

- You must only issue a refund to the original card that was used in the original sale

- You should never issue a refund by card where the original transaction was issued by another means of payment (such as cash)

- You should never issue a refund by cash or other means when the original sale was made by card

- You may only manually key a refund into a card machine if you have permission to process Card Not Present transactions

- You must never allow the transfer of money by refund to be processed onto your own card or those of your staff members

- You may not process a refund as a form of returned winnings unless specifically authorised to do so by AIBMS.

# 3. Card Security

## 3.1 Best Practice in guarding against fraud

To protect your business and your customers, it is vital that all staff understand the following guidelines, which aim to reduce the possibility of fraud and chargebacks.

### 3.1.1 Card Present

Cardholder Present transactions are generally considered secure because the cardholder must authenticate the payment using their PIN code. Where a payment is made by tapping the card, there are limits to the value of a transaction and to how many consecutive transactions can be made before the cardholder is required to authenticate the transaction. However, there are several things that are important to know:

- In a situation where a cardholder's card is blocked or an incorrect PIN is repeatedly entered, you should seek an alternative card or method of payment. You should not key in the card number manually when the customer is present, as this leaves you open to chargebacks.
- Always ensure that the customer does not interfere with the card machine. You should always keep the card machine in view of staff.
- Most cards have a chip and require PIN based authentication. If a card doesn't have a chip, or if the chip is damaged, the card machine should instruct the customer to sign for the goods. If this happens, you should ensure to:
    - Compare the card number on the card receipt with the physical card and ensure that they match.
    - Most cases of counterfeit fraud involve skimming, which means that genuine data from one card is copied onto another card illegitimately.
    - Check the signature on the back of the card matches the signature on the receipt.
    - Ask for identification and compare that with the name on the card.
    - Check whether the signature strip on the back is tampered.
    - Ensure that the card number on the physical card is embossed.
    - Be aware of these behaviours:
        - Does the cardholder appear nervous, agitated, or hurried, or are they trying to distract you by being rude or overly friendly?
        - Are they making indiscriminate purchases?
        - Are they making small item purchases with maximum value cashback?

You should never:

- Allow a customer to split a transaction across multiple cards.
  If the transaction amount exceeds your ceiling limit, you should contact AIBMS to have the ceiling limit raised.
- Key a transaction into a card machine when the customer is physically present.

What you should do:

- Immediately contact the authorisation centre and state that you have a code 10 authorisation.

### 3.1.2 Card Not Present

Processing Card Not Present transactions via a standard Chip & PIN machine are not recommended as they carry an additional level of risk.

As the card/cardholder is not physically present at the time of purchase, you cannot validate the legitimacy of the transaction.

**NB: You are fully liable for any chargebacks raised because of processing Card Not Present transactions.**

Where possible, always ask the cardholder to come to the store to complete their purchase as a Card Present transaction. Card Present transactions are generally considered secure because the cardholder must authenticate the payment using their PIN code.

If, however, you wish to proceed with a Card Not Present transaction, please ensure to capture the below information.

For all Card Not Present 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 billing address.
- The delivery address.

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

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, you should take the following precautions:

- Request to see a copy of the card at the premises that you are delivering the goods to.
- 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. You should keep an accessible record of the proof of delivery.

### 3.1.3 eCommerce

The way in which you handle your eCommerce website, and the associated transactions can have a major impact on the likelihood of transaction disputes arising. At all times, you should adhere to the following guidelines.

When a cardholder places an order, you must:

1. Provide details of the different steps that are required to conclude the sale and advise whether the contract of sale will be kept by you and made accessible to the cardholder.
2. Acknowledge receipt of the order to the cardholder, as soon as possible, by electronic means.
3. Make it easy for a cardholder to review their order prior to completing payment, to help them make any changes prior to completing the order.
4. Provide easy access to information regarding any relevant codes of conduct to which your business subscribes to and how these can be consulted.
5. Make it simple for cardholders to view and store any applicable terms and conditions.
6. Use of Secure Customer Authentication (3D Secure is the most common) wherever possible is required in many ecommerce scenarios and provides the cardholder and the merchant with the best security against fraud available.

When taking payment or providing a refund, you must:

1. Make payment options clear and provide simple instruction on how to complete payment.
2. Only process refunds to the card that was originally used for the purchase.
3. Secure your website in a way that is appropriate for sending personal and financial information, with a minimum standard of 128-bit key encryption.
4. Make policies concerning order cancellation, refunds, and other purchase conditions clear and transparent. You should also make it easy for a cardholder to contact you in the event that a refund or cancellation is required.
5. Make it clear to cardholders how and to whom they can make a complaint, and include a phone number, email address and postal address.
6. Provide a receipt for payment at the point of delivery.

When providing a receipt:

You must provide a receipt for all purchases. You may choose to provide this receipt in a digital or physical format, or both. When providing receipts, you must:

1. Ensure that all receipts contain the following information:
    a. The concealed card number
    b. A unique transaction identifier

c. Cardholder name
d. Transaction date
e. Transaction amount
f. Transaction currency
g. Authorisation code
h. Description of products or services
i. Your business name
j. The website address

2. Provide an online acknowledgement of the transaction and encourage the cardholder to retain proof of purchase for their own records.

When delivering goods or services:

1. Always record both the billing address and the delivery address, where they differ.
2. Ask the cardholder to review billing and delivery information prior to payment to ensure that they are correct.
3. Delivery dates and times should be made clear to the cardholder. In the event that a delivery date cannot be rescheduled to an appropriate alternative, the cardholder should be entitled to a refund.
4. Guarantee terms and details should be clearly stated. You should make it clear that any such terms will, in no way, affect their statutory rights. If there is a third party backing your guarantee, you should make the particulars of this third party clear to the cardholder.
5. Always retain proof of delivery, so that you can produce it in the event of a dispute.

Recurring payments enable you to capture payment details once, and then use this over time to charge fixed or variable amounts, as agreed with the cardholder, when providing their initial card details. You must seek permission from AIBMS prior to processing any recurring payments.

If you process recurring payments, you must:

- Ensure that any repeat authorisation attempts, following a decline, are limited to a maximum of one authorisation request per day and such requests must cease after 31 days.

## Security Guidelines:

By setting up an internet-based/Ecommerce payment facility with AIB Merchant Services, and as part of your merchant agreement, you must:

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.
4. Ensure that the electronic form used to process the transaction contains the following information:

a. Transaction amount
b. Card Type
c. Cardholder Number
d. Card expiry date
e. Cardholders full name
f. Cardholders billing address
g. Cardholders' delivery address

5. You should ensure that any sensitive data transmitted from the web browser to any server should be protected using a minimum of 128-bit SSL.
6. If you choose to host your website with a PCI-compliant ISP, you must ensure that any card data stored on the ISP's server is always encrypted.

**You must ensure that all transactions are processed using the minimum-security encryption standards.**

## Network Security:

- You should ensure that firewall technology and all associated minimum-security standards are in place between any servers involved in your online trading infrastructure
- You should ensure that appropriate traffic filtering elements are in place to prevent unauthorised access to your servers
- Your systems should be audited daily to identify any attempted or actual breaches of the integrity of the firewall
- The system must provide user authentication as required, including where necessary, token authentication

## Internet Service Security:

- The systems should 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
- An audit trail should be kept of all internet based transactions

## Backup

- All server data should be backed up on a regular basis, and all backup data should be stored at an offsite location
- Cardholder numbers should be purged from the server at least every 2 weeks

- Transaction details must be stored offline and securely for a minimum of 12 months from the date of dispatch of goods or provision of services
- You must ensure that under no circumstances, either on paper or on any system, are card security codes (CSC, CV2, CVV2) stored upon accepting card not present transactions

## 3.2 A Data Compromise Event

Data Compromise events are generally deliberate attacks on systems where cardholder data is stored, and can affect the systems of merchants, agents and third-party service providers.

All data held or transmitted is at risk of being compromised, and any weak links in these chains are typically targeted by fraudsters to steal sensitive information (such as card numbers and customers personal information).

A data compromise event can have a very detrimental effect on your business. Along with significant reputational damage, you could also incur card scheme fines. You would be required to use PCI Forensic Investigators and Qualified Security Assessors to ensure that all vulnerabilities have been secured and that PCI DSS requirements are met, which can be costly.

If you have a confirmed or suspected security breach, you must take immediate action by contacting the AIBMS customer support centre. Do not interfere with your systems in any way upon suspecting a data compromise, as a PCI forensic investigator will preserve any data found on your systems prior to carrying out investigation.

You can do your utmost to protect your business and your customers by being compliant with PCI DSS requirements. (see section 3.3 below)

## 3.3 Payment Card Industry Data Security Standards (PCI-DSS)

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 several 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.

### AIBMS PCI DSS Programme

It is a requirement for all merchants to report on their PCI DSS compliance. AIBMS have partnered with Sysnet Global Solutions to provide an online merchant portal to assist you in completing this process. https://www.aibmsdatasecurity.com/safemaker/login/portal

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 also be contacted on 1890 98 70 80.

## 4. Settlement, Statements and Reconciliation

Insight is a free and easy to use online tool that allows you to view and manage your AIB Merchant Services account, 24/7. You can use Insight to help you manage your settlements, statements, and to aid with bank reconciliation.

If you have multiple merchant accounts, these can be grouped together to allow you to view all information from within one system.

### 4.1 Settlement

AIBMS has several transaction processing windows, your processing window will be dictated by the card machine or online payment facility that you have. In some cases, you may be required to perform an end of day batch on your physical card machine.

Funds will be settled directly to your nominated bank account, in line with the respective banking calendar relative to your location. Please link in with your business development manager or relationship manager to discuss your funding set-up.

All payments will be made to you, net of any refunds processed. Please refer to the user guides available via Insight for more detail on how to view and reconcile your account.

### 4.2 Statements

Your AIBMS statement is available monthly via Insight. You can use Insight to find, view and download your statements in multiple formats.

Your statement provides you with the details of all applicable fees and charges and gives you an overview of your transactions, as well as checking for authorisations to see what has been approved or declined. You can find out more about Insight, and how to navigate a statement here: https://www.aibms.com/help/insight/about-insight/

### 4.3 Reconciliation

You can use Insight to quickly match the funds settled to your bank account, reducing time and effort associated with reconciliation.

You can search for funding amounts by date range, see the status of payment batches such as the day they were paid, and within each payment batch you can drill down into transactions to see applicable charges by specific card brand. Also, if you need to cross reference any of your payment batches with your bank statements, you can easily export them.

## 5. Chargebacks

A Chargeback is the return of funds from an already cleared transaction, processed on a credit or debit card, to the cardholders account. Chargebacks can be initiated by the customer's card issuing bank, at the cardholder's request, or if the issuing bank is required to do so under card scheme rules.

All merchants who accept card payments run the risk of being liable for chargebacks, and they can occur even where you have obtained authorisation for the transaction.

The most common chargeback reasons are:

- Fraud enquiries, where the cardholder denies making the transaction
- Disputes regarding a failure to receive the goods or services
- Disputes relating to quality of the goods or services

In card present scenarios, the cardholder is liable for fraud related scenarios if they have entered their PIN code. In card not present and eCommerce transactions, the merchant is liable if 3DS is not enabled on your website. When a transaction is disputed, it is important that you can provide as much information to connect the cardholder to the transaction. This will assist AIBMS in defending the transaction on your behalf.

Please refer to the AIBMS chargeback handbook for more information on preventing and handling chargebacks. www.aibms.com/help/chargebacks-fraud/dealing-with-chargebacks/

## 6. Managing your AIBMS Account

### 6.1 Changes to your business

Some changes in a business will result in a Change of Legal Entity (COLE)* or a change of legal name, which will take place if:

- The business undergoes a change of ownership
- New directors have joined the company
- Directors have left the company
- The business has changed entity type, for example, from a sole trader to a limited company or a limited company to a sole trader
- The legal name of the business has changed.

It is critical that you notify AIBMS of these changes to prevent issues arising after the change in your business has taken effect. Please contact our Customer Support centre in the event of any changes to your business taking place.

In the event that you have a terminal lease with First Data Global Leasing or MMSL (Clover), you must also contact them directly to advise them of this change.

*It is important to note that in circumstances where a COLE has taken place, there may be a requirement for a new Merchant ID (MID) to be set-up. If this is the case, an update is required on your card machine to reflect the new MID, to ensure your funds are deposited into the correct bank account.

## 6.2 Making a complaint

At AIBMS, 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 service you have experienced, we would like to hear from you and we will endeavour to make it right.

If you wish to make a complaint, you should first contact our customer service centre and outline the reason and details of your complaint. https://www.aibms.com/contact/
All complaints are thoroughly investigated, and we will keep you up to date on the progress of resolving your complaint.

If you are not satisfied with how we have dealt with your complaint, you may refer the matter to the Financial Services and Pensions Ombudsman, provided that you come within the jurisdiction of that body).

**ROI**
Lo-call Phone: 01 567 7000
E: info@fspo.ie
W: www.fspo.ie

**UK**
Lo-call Phone: 0800 023 4567 Fax: 0207 964 1001
E: complaint.info@financial-ombudsman.org.uk
W: www.financial-ombudsman.org.uk

## 6.3 Ending your Merchant Services Agreement

If you wish to terminate your AIBMS agreement, please refer to the termination provision in your terms and conditions.
If you have a card machine, you will be required to return this. Please contact the Customer Service team to arrange this. https://www.aibms.com/contact/

If you have a card machine provided by First Data Global Leasing or MMSL (Clover), you must contact them separately to discuss the terms of your termination, otherwise you will continue to be debited by them following the termination of your AIBMS agreement.
Please refer to your lease agreement for more information regarding termination of a lease.

# 7. Helpful Information

## 7.1 Global Choice (Dynamic Currency Conversation – DCC)

Your payment facility may be enabled for Global Choice. This enables your international customers to pay in their home currency, should they choose to do so. When an international card is presented, the cardholder will automatically be given the option to choose between paying in their home currency, or in the currency where payment is being taken. The relevant rates will be displayed to the cardholder. If they choose to pay in their home currency, this will be reflected on their receipt, and the transaction will be funded to you as normal. Each quarter, AIBMS will provide a commission share to you on any applicable Global Choice transactions, as a rebate on your monthly statement.

## 7.2 Manual Fallback Solutions

If your card machine fails, please contact the terminal support helpline noted on the sticker on your machine and we will arrange a remote resolution or a replacement as soon as possible.

If your machine needs to be replaced, you can avail of one of our fallback options while you await the delivery of your replacement:

- Manual Vouchers
- Virtual Terminal

Both systems will allow you to continue to process card transactions while you await your replacement. Please ask our terminal support team for more information (details noted on the sticker on your terminal).

### 7.2.1 Manual Vouchers

Please ensure to print a sufficient quantity of the vouchers to cover your card payment needs until such time as your terminal issues are resolved. https://www.aibms.com/help/terminal/sales-vouchers/

Please note, when taking manual vouchers, great care and attention is required. Please follow the guidelines noted below and share this information with all staff members at your premises:

- Manual vouchers can **NOT** be used for the following card types:
  - Maestro/ International Maestro
  - Visa Electron

Please note, if you do attempt to manually process transactions for these card types AIB Merchant Services cannot guarantee payment, even if authorisation is given.

- Manual vouchers should not be used for refunds

- Before commencing the transaction, you can ask the cardholder if they have any form of ID to substantiate them as the genuine cardholder.
  This is not mandated but it will give you a greater degree of confidence that they are not attempting to commit fraud.

- Please complete the manual voucher template with the following details:
  - Full Card Number
  - Expiry date
  - Cardholder Name

- Merchant Name
- Merchant Identification Number (MID)
- Transaction Date
- Transaction Description
- Transaction Value
- Authorisation Code – to gain a manual authorisation, please call us on the relevant number below (please be sure the cardholder is present):
  ROI 01 247 6544
  UK 0345 604 1625

*Please note, successful authorisation is never a guarantee of payment. An Authorisation only confirms the card has not been reported lost/stolen and there are adequate funds for the requested transaction.

- Please ensure the card holder signs the manual voucher
- Confirm the signature matches the signature on the reverse panel of the card
- Confirm the name signed matches the embossed name on the front of the card
- **If any of the cardholder's information does not match, you should stop the card transaction immediately and insist on another form of payment**

When your terminal is operational again, please collate all vouchers and send via a secure method (i.e. registered post) to the relevant address below:

**ROI**
AIB Merchant Services
Collections Department
10 Hanover Quay,
Dublin Docklands,
Dublin 2, D02 A3W8.

**UK**
AIB Merchant Services
PO BOX 288,
Sheffield,
S98 1SA.

We will then rekey the transaction on your behalf. The funds will be settled to your account in line with your normal funding schedule.

Chargebacks

Please be aware that using manual vouchers (as with any non-secure transaction) will put you at risk of chargebacks. In the event of a chargeback being raised, you will be fully liable for any charges applied.

To find out how businesses can best protect themselves against Chargebacks please refer to the chargeback section above (see section 5).

### 7.2.2 Virtual Terminal (VT)

To avail of a temporary VT, you will need access to a PC, laptop or tablet at your point of sale to allow you key in the card details in front of the cardholder.

Chargebacks

Please be aware that using a Virtual Terminal (as with any non-secure transaction) will put you at risk of chargebacks. In the event of a Chargeback being raised you will be fully liable for any charges applied.

To find out how businesses can best protect themselves against Chargebacks please refer to the chargeback section above (see section 5).

## 7.3 Promoting Card Acceptance

We recommend promoting your acceptance of card payments in your premises and on your website. For card present solutions, we include some branded decals in the box you received your card machine in. You can order more by contacting our customer support team. https://www.aibms.com/contact/

When promoting card acceptance, you must adhere to the brand guidelines set out by each card scheme. You can find out more information regarding these brand guidelines here: https://www.aibms.com/help/working-with-aibms/card-schemes-and-useful-websites/

## 7.4 Accessories

You can purchase accessories for your card machine, including paper rolls and cleaning materials at www.aibmsaccessories.com.