Elavon

UK Operating Guide

Table of Contents

Section 1 – Introduction

Welcome to our Operating Guide. We would like to take this opportunity to thank you for selecting Elavon as your acquirer and assure you that we will endeavour to provide the most efficient and professional service at all times.

We want you to be totally comfortable and familiar with your Card acceptance programme to allow you to maximise its value to your business.

This Operating Guide (the "Guide") forms part of your Agreement with us. It has been designed with particular reference to point-of-sale procedures. It is important that all of your staff dealing with Card payments are familiar with the point-of-sale procedures in this Guide.

We have produced this Guide, which sets out to answer the questions most frequently asked by Customers. If you have requested a Terminal, you will also receive a Quick Reference Guide. If you have any queries not covered by either the Guide or the Quick Reference Guide, please do not hesitate to contact us – our contact details are located on the back cover of this Guide.

Unless specifically defined in this Guide (including in Section 13 – 'Glossary'), capitalised words and phrases used shall have the same meaning as set out in the Terms of Service forming part of your Agreement with us.

For additional information please refer to our website **www.elavon.com**.

Section 2 – Authorisation

2.1 Automated Authorisation Service

Authorisation can be sought by telephoning the Authorisations centre (on the number appearing on the back cover of this Guide). Once connected you will hear the following menu options:

- for authorisation on a card, **press 1**
- for a code 10, **press 2**
- for a name and address check, **press 3**
- for an authorisation reversal, **press 4**
- for help menu option, **press 5**

If you not respond within 5 seconds, you will be transferred to the next available Agent.

Authorisation Code:
Please key this code into your Terminal or write it in the designated box if using a paper voucher.

Declined Response:
Please advise the Cardholder that the Transaction has not been authorised. An alternative payment must be sought.

Referral:
Your call will be automatically transferred to an agent where they will talk you through the next steps.
If the Cardholder queries a response, please advise them that they must call their Card Issuer directly. An Authorisation Code confirms that, at the time of the Transaction, the Card has not been reported lost or stolen and that there are sufficient funds in the account to which the Card relates.

Take Imprint of Card:
Please follow the manual sale procedure set out below if your Terminal ceases to work or prompts you to take an imprint of the Card and you possess an imprinter. In such instances, please read the instructions set out in Section 6 of the Guide.

Pre-Authorisation Request:
For information on how to perform a pre-authorisation please refer to your Quick Reference Guide.

2.2 When to use a Code 10 call option

1. The Cardholder's signature differs from that on the Card.
2. The title on the Card does not match the person presenting the Card.
3. The Card has not been signed.
4. The signature strip has been violated or the Card has been otherwise damaged.
5. You have reason to be suspicious about the validity of the Card, the Transaction or the person presenting the Card.

Hold on to the Card and the goods to be purchased and/or ensure the services are not provided, whilst you contact the Authorisations centre.

2.3 Card Acceptance/Checking a Card

The following details must always be checked each time you accept a Card for a payment, even if the Cardholder is one of your regular customers and is known to you.

1. Start date (if available): Check that the start date on the Card is not in the future. Cards with start dates in the future must not be accepted.
2. Expiry date: Check that the expiry date on the Card has not passed. Expired Cards must not be accepted.
3. Cardholder's name: Check that any title on the Card agrees with the person presenting it, e.g. that a Card issued to a woman is not presented by a man.
4. Signature panel: Check that the Card is signed and that the signed name agrees with the name embossed on the front of the Card. Also, check that the Cardholder's signature on the Transaction Receipt is not written hesitantly or printed and corresponds with the signature on the Transaction Receipt. When you are holding the Card, rub your thumb over the signature strip, which should be smooth and flush.
5. Account number: Check that the account number embossed on the Card matches any account number appearing on the Card's reverse side.

You will not accept a Card if any of the above checks has failed.

If you submit a Transaction from a Card bearing the logo of a Card Scheme that you are not permitted to accept, the Transaction will be rejected and returned to you. You may not process Card Not Present Transactions unless we have agreed in writing that you may do so.

2.4 Authorisation Code

You must obtain an Authorisation Code before completing any sales Transaction, whether electronically though use of a Terminal or verbally by telephoning for an Authorisation Code. You must provide the following information to obtain an Authorisation Code for all Transactions:

(i) Customer Bank Account number;
(ii) Card name and number;
(iii) Card expiry date;

(iv) Amount of Transaction;
(v) Date of Transaction;

and for MO/TO Transactions only, the following in addition:
(vi) CVV2/CVC2 number;

and for Internet Transactions only, the following in addition:
(vii) CVV2/CVC2 number;
(viii) confirmation that the Transaction has been authenticated using 3D Secure™;
(ix) Customer's URL address.

Authorisation Restrictions on Internet Transactions
In relation to Internet Transactions only, the following restrictions apply on obtaining Authorisation:
(i) For goods to be shipped, you may obtain Authorisation on any day up to seven (7) days prior to the Transaction date, being the date the goods are shipped. This Authorisation is valid if the Transaction amount is within fifteen percent (15%) of the Authorisation amount, provided that the additional amount represents shipping costs or such other costs as are permitted by the Rules.
(ii) You may not enter into a Transaction at any time where you receive the Cardholder's details via the internet and then enter the Cardholder's details into a Terminal manually.
(iii) You will follow any instructions received during Authorisation. Upon receipt of an Authorisation Code, you may complete only the sales Transaction authorised and must ensure that the Authorisation Code is noted on the Transaction Receipt.

2.5 Cardholder Authority

Nothing in the Agreement, including receipt of an Authorisation Code, precludes you from the requirement to obtain authority to debit the Cardholder's account for each Transaction. Such authority shall be deemed given (unless the Card is reported lost, stolen or compromised):

1. For Card Present Transactions, by obtaining a signed Transaction Receipt or in the case of a PIN Transaction, the printed Transaction record produced by the Terminal.
2. For Mail Order Transactions, by obtaining the signed written authority of the Cardholder.
3. For Telephone Order Transactions by retaining documentary evidence of the Cardholder's authority to debit his/her account for the amount of the relevant Transaction.
4. For each Mail Order/Telephone Order Transaction, you must keep and produce to Elavon on demand, documentary proof of dispatch of the goods or supply of the services rendered for not less than two (2) years from the Transaction date.
5. For Internet Transactions, by obtaining the CVV2/CVC2 number from the Card.
6. For Contactless transactions, the Contactless reader display will confirm the transaction has been successful; there will be an audible success tone and a visual indication (lights and/or an 'Approved' message on the display). Where applicable the terminal will print a receipt - confirming that the transaction has been successful and is complete.

Please remember authorisation is not a guarantee of a payment.

Section 3 – Electronic Processing

Please note that you are not allowed to refund the cash amount when a purchase has been made with Cashback.

- Ensure your Terminal is set to the correct date and time.
- Follow the guidelines set out in Section 2.3 – 'Card Acceptance/Checking a Card' – of this Guide.
- Ensure the Transaction type identified by the Terminal is correct.
- Ensure the number embossed on the front of the Card matches the number printed on the Transaction Receipt.
- Swipe or insert the Card into the Card Reader or present the card (for a contactless transaction).
- Obtain Authorisation in accordance with Section 2 – 'Authorisation' – of this Guide.
- If the Cardholder has signed the Transaction Receipt ensure the signature corresponds to that on the reverse of the Card and that all written details have copied through to the bottom copy of the Transaction Receipt.
- When you are confident that everything is in order, give the Cardholder a copy of the Transaction Receipt, return the Card, and hand over any goods.
- Please retain the top copy of the Transaction Receipt (transaction receipts should be retained for a minimum of two (2) years.

The Transaction is now complete.

3.1 PAN Key entry

If the Card is unsuccessfully swiped, the Chip cannot be read or a Terminal Card reader is not working, a message will appear on the Terminal confirming the Card has not been read successfully. If you have been provided with the PAN Key entry facility, the following procedures should be followed:

- The Terminal will prompt you to enter the Card details which will include:
  (i) Card number (PAN): the 13-19 digits Card number embossed on the front of the Card;
  (ii) Expiry date.
- You will be prompted by the Terminal to 'Enter' the Transaction.

An imprint of the Card should be taken on a paper voucher to prove that the Card was present and the Cardholder was asked to sign the paper voucher. Please ensure that a description of the goods, the amount and the date are also captured on the paper voucher. This will help to reduce the risk of error and therefore minimise your exposure to Chargebacks.

The paper voucher must be kept with your copy of the Transaction Receipt. If you do not have the PAN Key entry facility, the Transaction should be accepted on a paper voucher. Please refer to Section 6 – 'Back-up Procedures – Paper Vouchers' – of this Guide.

3.2 Submission of Transactions

Please note that the end-of-day banking process should be carried out every day on which Transactions are accepted to avoid any late presentation charges. You should submit the data captured on your Terminal within 48 hours of the Transaction completion. Any Transactions submitted after this time will be downgraded by the Card Schemes and may attract an additional charge (see section 11).

3.3 Chip and PIN Cards

Incorrect PIN/Blocked PIN: If the Cardholder has entered the wrong PIN three times, the PIN is blocked.
The Cardholder should be advised to contact their Card Issuer. The Transaction will attempt to proceed as Chip and signature via Authorisation. If this is permitted, then perform the usual checks that you would for any signature Transaction. Be extra vigilant if a blocked Card is presented. If a PIN is entered correctly but you continue to be suspicious of the Cardholder, make a Code 10 call to the Authorisations centre.

Faulty Chip Cards: If the Terminal Card reader cannot read the data on the Card, the Terminal will usually prompt three times to use the Chip reader. If this is still unsuccessful after three attempts, the Terminal will default to a magnetic stripe Transaction. If this occurs then perform the usual checks that you would for any signature Transaction.

3.4 Contactless Cards

Contactless is a feature on payment cards to make low value purchases quicker and more convenient for both retailers and consumers. When making low value payments - rather than inserting a card into the chip & PIN machine and typing in a PIN – those with a card featuring Contactless can simply hold it to the reader to pay.

How do I recognise a Contactless card?
Cards featuring Contactless will look much the same as a standard chip and PIN card, but will have been re-issued with a new design incorporating one or more contactless identifiers. The majority of cards issued in the UK will feature the contactless indicator:

Contactless identifiers may be found either on the front or the back of the card

Section 4 – Statements

4.1 How to read your Statement

A statement is sent to you daily, weekly or monthly in accordance with the Agreement. This shows the total of all Transaction batches by way of a Summary of Charges ("SOCs") that we have processed on your behalf in the previous settlement period for Credit Card and Debit Card Transactions, the amount credited to your Customer Bank Account, and the Merchant Service Charges (MSC) that is due for payment.

Any Transaction batch received by us that is found to be incorrect or invalid will be advised to you separately. Based on the payment summary (see point 4 below), your Customer Bank Account will either be credited or debited, in normal circumstances, shortly after you receive your statement, with the payment amount shown on your statement.

A sample statement appears on the left-hand page. Below is an explanation of some of the key information that will appear on your statement.

1. **BILLING PERIOD**: Shows the billing period covered by the statement.
2. **PAYABLE**: Shows the final amount that will be debited from your account. It also shows the last four digits of the Customer Bank Account number from which the amount will be debited.
3. **SUMMARY**: Transactions Summary – this is a summary of transactions we have settled to you by transaction type, number and amount. The Total GBP Amount is the amount we deposit to your Customer Bank Account (see section 11 below).
4. **FEES SUMMARY:** – this is a summary of fees total payable by you (as further explained in sections 4 – 8 below).
5. **REBATES**: Shows rebates made on your account during the month, for example Dynamic Currency Conversion (DCC).
6. **CARD FEES**: Description – this section shows the total Merchant Service Charges payable by you by card type and volume of transactions. The base rate agreed for each card type is under the column "Discount Rate". Any card types charged per item will be displayed under the column "Per Item Rate".

   Exception Description – an exception fee is a charge that occurs for Business Card transactions and for transactions which were downgraded. Downgraded transactions are generally higher risk credit or debit transactions and include non - Chip and PIN, manual keyed and non-secure internet transactions. These transactions will be listed on your statement as Business Cards, Credit Exception, Maestro UK Debit Exception or Visa Debit Exception.
7. **OTHER TRANSACTION FEES**: Any other fees applicable to your Customer Bank Account will appear in this section.
8. **ACTIVITY FEES**: This section shows fees applicable to your Customer Bank Account for Example; Authorisations by card type (IP AUTH).
9. **OTHER FEES**: Other fees such as terminal rental will be included in this section and here relevant, VAT will be charged in addition.

   Other fees can include:

   A) Equipment fees – you will be charged for any hardware (Terminals/PDQ) that you have on your premises – these will be charged at a per unit rate and will have VAT applied where applicable.

   B) Statement Fee – While we strongly recommend that you avail of our free of charge on line statements, if you wish to receive these by post there is a fee for this.

   C) PCI Non Compliance – if you are not compliant with PCI and have not become certified within the mandated timeframe you may incur PCI non-compliance fees. To reduce your monthly spend and to cease this fee immediately please ensure to become PCI compliant.

   D) Terminal Upgrade fees – If any time you have taken the decision to upgrade your current hardware to a higher spec or newer model an upgrade fee will be charged for this – this will have been agreed during your initial conversation with one of our customer care team.

10. **CHARGEBACKS /REPRESENTMENTS**: Any transactions still subject to chargeback or representment within the billing period are set out in this section.
11. **ADJUSTMENTS**: This section details any adjustments required to be made to your Customer Bank Account within the billing period.
12. **DEPOSITS**: This section shows all transactions received ("Batch") during the billing period which have been processed by Elavon. The "Funded Amount" is the amount that will be credited to your Customer Bank Account. The "Payment Number" and the "Funded Amount" figure will correspond with the reference and amount that appears on your bank statement.

Please note that you will receive separate statements for your Transaction in respect of Diners, JCB and American Express Cards.

We strongly recommend you use iMerchantConnect our online reporting and statement tool where you can access your statements.

4.2 How Card Payments Work

A Card Transaction involves the following steps:

- The Cardholder is granted a line of credit by the Card Issuer. This allows the Cardholder the facility to spend up to a predetermined amount each month. American Express Charge Cards do not have a pre-set spending limit.
- You, as our Customer, are approved for Card acceptance and an account is opened for Card Transaction processing.

When you accept a Card as a form of payment, the Transaction value is credited to your Customer Bank Account. Details of the Transaction are then sent to the Cardholder's Issuer, where the amount is debited from his/her account. This transfer of funds normally occurs within three (3) Business Days and will be listed in the statement of both parties – a credit appears on your Statement and a corresponding debit on the Cardholder's account statement.

Transaction flow: The Transaction and the transfer of value flow from your Terminal to an Acquirer, to the Cardholder's Issuer and finally to the Cardholder's account. Acquirers receive payment in the opposite direction and transfer the value to your Customer Bank Account. During this process the Transaction has travelled through the Card Schemes processing networks, which cover the entire world. This entire procedure is called "Settlement". Our Merchant Service Charges are deducted from your submitted Transaction batches, along with any other adjustments, such as corrections or Chargebacks.

Section 5 –Fraudulent Transactions

The following Card Acceptance Types are covered in this section under:

- **5.1 Card Present Acceptance**
- **5.2 Card Not Present Acceptance**
- **5.3 Fraud – "Code 10"**
- **5.4 Card Recovery**
- **5.5 Know Your Staff**
- **5.6 System Security**
- **5.7 MasterCard Secure Code/Verified by Visa (3D Secure)**

5.1 Fraud – Card Present Acceptance

Card present occurs when a card is present at the time of the sale; merchants are required to take all reasonable steps to ensure that the card, cardholder and transaction are legitimate.

CUSTOMER GUIDE TO SAFEGUARDING CHIP TRANSACTIONS

ACCEPTING A CHIP CARD

For chip and pin transactions; the card is inserted in the terminal and the card holder must enter a PIN, instead of signing a paper receipt. The terminal authenticates the card, based on comprehensive and secure information contained on the chip. The terminal also verifies the identity of the card holder, based on the PIN.

The process to perform a chip and pin transaction is similar to a magnetic strip transaction.

1. Either you or the customer enters the chip card into the pin pad
2. After the card has been read you enter the amount on the terminal
3. The customer then enters their pin using the pin pad
4. The terminal will then verify the transaction

For chip and pin transactions; no signature is required and the receipt will state that the transaction was 'VERIFIED BY PIN'. Transactions not verified by pin will generally require signature, however, the terminal will advise if this is the case.

Guidelines to Safeguard Chip Transactions

- A Cardholder must never disclose their PIN to you, and you should always look away whilst the PIN is being entered. There are various PIN Pad designs with additional shielding around them but always encourage the Cardholder to shield the PIN Pad when entering the PIN. Other persons in the queue should also be encouraged to be mindful of those entering their PIN and must stand away from the till point.
- When presented with a Chip Card, always use PIN verification rather than a signature. Please note that if the pin verification process is bypassed, liability could shift from the card holder back to the merchant.
- Accepting a Non Chip Card, if you have a Terminal, advise all your staff that a manual imprint must only be taken for Cards where the Terminal cannot read the magnetic stripe/chip or the Terminal ceased to work. The Cardholder must sign the imprinted paper voucher and Authorisation must be obtained.

Guidelines to Safeguard Non Chip Transactions

- Do not process Card Not Present Transactions. Check the details on the Card:
  - Check that the expiry date on the Card has not passed, and also check that the start date (if available) is not in the future.
  - Check the Cardholder's name – make sure the title agrees with the person presenting the Card (e.g. that a Card issued to a woman is not presented by man).
  - Check to make sure the Card is signed and that the name is the same as that embossed on the front of the Card.
  - Check that the Card has a magnetic stripe and that the Credit Card logo is shown on the Card e.g. MasterCard, Visa, American Express and that the hologram (if present) moves/changes.
  - For American Express Cards, make sure that there are four digits printed on the front of the Card to the right-hand side above the Card number. Ensure that this number cannot be rubbed off.
  - Check the signature on the receipt matches the signature on the Card (if the Card is not a Chip Card).
  - Check the Card details imprinted on the Transaction Receipt match what is imprinted on front of the Card. Please refer to Section 5.3 – 'Fraud – Code 10' – of this Guide for reasons to be suspicious.

Accepting A Contactless Card

- When making payments below the contactless limit, a card featuring Contactless technology can simply be held to the reader to pay - rather than inserting a card into the chip & PIN machine and entering a PIN. In just a few seconds the payment will be complete and the lights on the reader will illuminate, confirming that the transaction has been approved.
- Contactless cards are secured by the same advanced technology that underpins chip and PIN. Although a Contactless transaction does not require a PIN to be entered, from time to time the terminal will ask that the cardholder to undertake a full contact chip and PIN transaction. This is designed to deter fraudulent use should the card be lost or stolen; each time a PIN is used it re-affirms that the cardholder is in possession of their card.

5.2 Fraud – Card Not Present Transactions

Before accepting any Card Not Present Transaction, please ensure your Agreement allows you to do so. You must take the necessary precautions to safeguard any such Transaction and help reduce the risk of a Chargeback arising. Most losses are generally experienced by Customers as a result of Card Not Present Transactions. Mail Order/Telephone Order Transactions are high risk, and you retain full liability should a Transaction prove to be fraudulent or not authorised by a Cardholder.

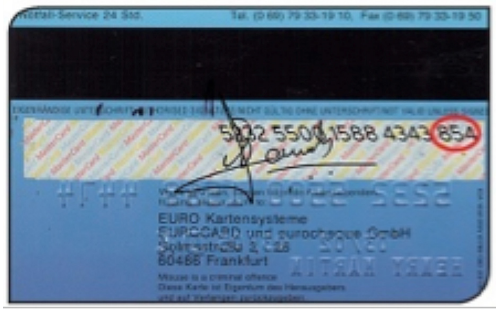
Watch out for:

- Multiple Transactions from the same Card number.
- Multiple Transactions from the same country or issuing bank, i.e. multiple Transactions where all the card numbers begin with the same six digits. It's the same four digits in the case of American Express Cards. Multiple use of the same Card number in a short time span.
- Multiple Transactions from the same address or area.
- Sharp increase in turnover/sales requests.
- High volumes of goods which are easily re-sold e.g. televisions, DVDs, hi-fi systems, computers.
- Transactions/orders from other countries which may appear unusual.
- For all Mail Order or Telephone Order transactions why not call the Authorisation centre to have an Address Verification Service (AVS) carried out.

For internet/ecommerce Customers the adoption of 3D Secure has the potential to greatly reduce the risk of fraud (see section 5.7).

Tips to help prevent fraudulent transactions:

- Only process a Refund on the Card on which the original Transaction took place. DO NOT refund a Card where the original payment was accepted by other means e.g. cash or cheque.
- Goods should never be given to taxi drivers, couriers or chauffeurs at the request of a Cardholder. Goods should be delivered to the Cardholder's address; care should be taken if delivering to a different address other that the Cardholder's billing address.
- DO NOT process Transactions for any other business than your own.
- DO NOT process any Transactions on a Card issued in your name or of a director or partner of the business.
- Verify the address for high-value Transactions – only forward goods to the billing address. Take a telephone number, address and check details against an electronic register or telephone directory.
- Get the Cardholder to provide the 3-digit Card Verification Code (CVV2/CVC2) listed after the Credit Card number on the reverse of the Card.



- For American Express Cards, request the Cardholder to provide the four digits printed on the face of the Card to the right-hand side above the Card Number (Card Identification - CID). You will need this information if you are suspicious of the Transaction.

IF A CARDHOLDER ASKS TO PICK UP THE GOODS, PLEASE TREAT THIS AS A CARD PRESENT TRANSACTION RATHER THAN A CARD NOT PRESENT TRANSACTION I.E. ENSURE TO PROCESS THE TRANSACTION AT THE TERMINAL WHEN THE CARDHOLDER IS PRESENT

5.3 Fraud – 'Code 10'

Responsibility for any fraudulent Transactions lies with you. The Code 10 procedure is designed to help reduce the use of fraudulent Cards. Authorisation does not guarantee payment, however, there are many reasons that can prompt you to be suspicious and take steps to avoid being a target of fraud such as:

- A Cardholder is hesitant when signing the paper voucher.
- A Cardholder provides you with a second Card in a different name.
- A Cardholder provides more than one Card number to cover one order or set of orders.
- A Cardholder appears disinterested in price or precise description of the goods.
- A Cardholder appears nervous and in a hurry.
- A Cardholder suggests splitting a sale into two or more separate sales.
- A Cardholder appears to be quoting someone else's Card details e.g. a male presenting a female's Card details.
- A Cardholder purchases the same product several times.
- A Cardholder is trying to distract you.

IMPORTANT:
A Code 10 is only used for Card Present transactions.
For all Card Not Present Transactions request an AVS check.

For further information on the above, please contact our Customer Service Team (on the number appearing on the back cover of this Guide).

If you are suspicious of any Transaction regardless of whether the Transaction is Card Present or Card Not Present - please contact your local Fraud Management Team for guidance and support on the following numbers:

Telephone Number +353 (0)402 25424
Fax Number +353 (0)402 26751

5.4 Card Recovery

You will use reasonable means to recover any Card:

(i) if you are advised by Elavon or instructed to do so by a Terminal, the Issuer, or a voice authorisation centre to retain it;
(ii) if you have reasonable grounds to believe the Card is lost, stolen, counterfeit, fraudulent, or otherwise invalid, or its use is not authorised by the Cardholder;
(iii) with respect to Visa branded and MasterCard® branded Cards, if the four digits printed below the embossed account number do not match the first four digits of the embossed account number; or

If this happens, do the following:

1. If the Cardholder is present when you are advised to retain their Card, advise him/her that their bank requests that the Card be retained and returned to them. If the Cardholder has any questions, he/she should contact their Card Issuing bank directly.

   Please note that you are not expected to endanger your own safety or that of other members of staff when retaining a Card.

   If the Cardholder is not present when you are advised to retain their Card, please advise him/her to contact their bank, as you are unable to authorise the Transaction.
2. Cut off the bottom right-hand corner of the Card taking care not to destroy the embossed Card number or magnetic stripe. This should be done discreetly and not in front of the Cardholder.
3. Please return both parts of the Card together with the Terminal receipt stating to retain the Card or a note of the reference code issued by the Authorisations centre agent, your Merchant ID, the name and telephone number of the person responsible for recovering the Card to:

Elavon Merchant Services
Card Recovery Section
PO Box 466
Brighton
BN50 9AW

Note: Rewards will only be payable once Elavon deem all necessary criteria have been met: (a) the 'Retain Card' request was issued either by the Terminal or by an Authorisations centre agent and (b) the Terminal receipt stating to retain the Card or the inclusion of the reference code issued by the Authorisations centre agent, are provided to Elavon.

For additional information on Card Security visit
www.elavon.com/acquiring/united-kingdom/merchant/card-security.aspx

5.5 Know Your Staff

- Obtain and check references for all staff hired including temporary and short term cover.
- Ensure accurate staff records are maintained and individual employee IDs are provided.
- Ensure to monitor and maintain staff shifts or rotas.
- Ensure full training is given to all staff on accepting Card payments.
- Complete audit checks from time to time to ensure that correct procedures are being adhered to, e.g. employees are using their individual IDs and not those of fellow employees.

5.6 MaintenanceSystem SecuritySecurity

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

5.7 MasterCard Secure Code/Verified by Visa ("3D Secure")

3D security is a security process that helps secure Card Transactions, and has also helped to address Cardholders' concerns about online shopping.

3D Secure verifies card authorisations by validating the Cardholder's identity through the use of a unique personal code. Once this is established 3D Secure will send you a response indicating that you may proceed with the Transaction

Section 6 – Back Up Procedures - Paper Vouchers

Please follow the manual sale procedure set out below if your Terminal ceases to work or prompts you to take an imprint of the Card and you possess an imprinter. Please note this form of Card processing should only be used as a backup if your Terminal is not working and you cannot wait for it to become available again or the Terminal prompts you to take an imprint of the Card because the magnetic stripe on the Card cannot be read.

There are no floor limits for manual sales, which means that you must contact the Authorisations Centre and obtain an Authorisation Code for all manual sales before continuing with the Transaction. Please refer to Section 2 – 'Authorisation' – of this Guide for guidance on how to obtain Authorisation via the Authorisations Centre.

Manual Sale Procedure (Card Present):

- Request Cardholder's Card.
- Contact the Authorisation Centre to obtain an Authorisation Code.
- Insert the Card face up in the Imprinter and insert the paper voucher for either sale or Refund, above the Card.
- Operate the Imprinter by sliding it firmly from left to right and back again to the starting position.
- Remove the paper voucher and check that all copies have been imprinted clearly with the full Card details and your Merchant information. (Merchant number, Merchant name (DBA), Merchant address)
- Remove Card from Imprinter.
- Complete the paper voucher (see instructions below) using a ballpoint pen. The Authorisation Code received from the Authorisations Centre must be entered on the paper voucher.
- Retain the Card and watch the Cardholder sign the paper voucher. Check that the signature is the same as that on the reverse of the Card.
- Check again that the details are correctly entered and appear on all copies of the paper voucher. If they do not, securely destroy the paper voucher and start again.
- When you are satisfied that everything is in order, give the Cardholder the top copy of the paper voucher and return the Card.
- Retain the remaining copies of the paper voucher in a secure place until you can process it electronically through your Terminal.
- Once the Terminal becomes available again, please re-enter the Transaction using the force or offline procedure. Please refer to your Terminal manual for details.
- If you are not able to re enter the transaction using force option or offline procedure, you need to force the transaction when the terminal is back online.

How to Force Sale/Offline Mode

1. Press the 'F' key to start the payment application, using the Up/Down arrows to scroll through the menu screens, select the NEW TRANS menu option and press ENTER
2. Select FORCE and press ENTER
3. Insert Chip Card (into PIN Pad where present, otherwise insert in the terminal chip reader) or SWIPE/KEY the number into the terminal. If keying, you will be asked for the Card Expiry Date also
4. Enter the FORCE amount and press ENTER
5. The terminal will prompt to key in the AUTHORISATION CODE received over the phone, and press ENTER
   Note: press key stroke quickly to enter the alpha characters
6. If a Chip Card, hand the terminal to the cardholder to enter their PIN (where PIN Pad is present, request the cardholder to enter their PIN)
7. Remove merchant copy receipt by tearing
8. If required, OBTAIN and VERIFY the cardholder's signature on the merchant copy
9. Press ENTER
10. Finally, a cardholder copy receipt is printed

How to complete a Sales Voucher

1. Cardholder's signature
2. Authorisation Code: Complete when authorisation is obtained
3. Insert the total value of the Card Transaction
4. Insert details of the goods/services purchased
5. Insert the Transaction date

Refund Vouchers are completed in the same way.

Section 7 – Chip and PIN – Contactless

Chip and PIN
Chip and PIN is the usual way to accept card payments on your terminal when the card and cardholder are present (some cardholders will still have magnetic stripe only cards and these must not be refused at the point of sale).

A Chip Card contains a microchip, which is embedded into the Card. It contains extremely secure memory and processing capabilities. The information it contains helps ensure that the Card is authentic and makes it difficult and expensive for a criminal to counterfeit the Card.

Chip cards have a contact plate like this:

A PIN is entered by the Cardholder to confirm that they are the actual owner of that Card. The PIN removes the need for the Cardholder to a sign a paper Transaction Receipt.

A CONTACTLESS CARD will look much the same as a standard chip and PIN card, but will have been re-issued with a new design incorporating one or more contactless identifiers. When making contactless payments, a card featuring Contactless technology can simply be held to the reader to pay - rather than inserting a card into the chip & PIN machine and entering a PIN. In just a few seconds the payment account information is communicated wirelessly (via radio frequency (RF)) and the payment will be complete and the lights on the reader will illuminate, confirming that the transaction has been approved.

Contactless cards are secured by the same advanced technology that underpins chip and PIN. Although a Contactless transaction does not require a PIN to be entered, from time to time the terminal will ask that the cardholder undertake a full contact chip and PIN transaction. This is designed to deter fraudulent use should the card be lost or stolen; each time a PIN is used it re-affirms that the cardholder is in possession of their card.

Section 8 – Chargebacks

8.1 Chargebacks

A Chargeback may occur for any of the reasons set out in Section 8.2 –'Circumstances that may result in a Chargeback being raised' – of this Guide A Chargeback will be raised by the Card Issuer as soon as the Card Issuer becomes aware of a suspicious Transaction. However, the time period for raising a Chargeback can be as much as 540 days from the Transaction date.

Any Chargeback queries should be addressed to the Chargeback Department at:

United Kingdom	**(0044) 0845 850 0195, option 4**	**0845 600 2465**	**chargebacks@elavon.com**
Ireland	**(00353) 0402 25020, option 4**	**0402 25610**	**chargebacks@elavon.com**

8.2 Circumstances that may result in a Chargeback being raised

- Chargeback may occur when a Card Issuer returns an unpaid Transaction because they consider the Transaction to be invalid or unauthorised by the actual Cardholder.
- Split sale – If you split a high-value sale into two or more amounts that are below the floor limit to force the Transaction through without checking for Authorisation on one high-value Transaction amount.
- If the Customer's Terminal requested that the Customer call for Authorisation but the Transaction is forced through without calling the Authorisations centre. Alternatively if the call is made but Authorisation is declined and the Transaction is still forced through.
- The amount processed by the Customer exceeds that authorised by the Cardholder.
- Duplication – If the Cardholder was charged for the same transaction more than once.
- Expired Card – If the Customer process a Transaction with an expired Card.
- No Transaction Receipt – If the Cardholder's Card Issuer requests a copy of the paper voucher and the Customer is unable to provide sufficient signed/imprinted documentation to prove the Cardholder actually participated in the Transaction. Paper vouchers/Transaction Receipt copies must be kept by the Customer for at least two (2) years from the Transaction date.
- If the Customer cannot provide written evidence of a Transaction having taken place within the time limits set by the Card Schemes.
- Refund not processed – If the Cardholder has written evidence that the Customer agreed to process a Refund but has not received the Refund.
- Failing to take an imprint of the Card at the time of the Transaction or failing to get the Cardholder to sign a paper voucher.
- Late presentation – If a Transaction is processed by the Merchant beyond the three (3) Business Day time limit.
- A Card account number was incorrectly manually entered into the Terminal or handwritten on a paper voucher causing the Transaction to be processed to an invalid/incorrect Card account.
- Cancelled recurring Transaction – If a Cardholder has written evidence that they have cancelled a mandate/subscription with the Customer but the recurring Transactions are still being processed to his/her account.
- Credit posted as purchase – If the Customer puts through a Refund but it is processed as a sale, therefore debiting the Cardholder account again. This Chargeback is for twice the Transaction amount.
- Goods not as described – If the Cardholder has a picture or written description of an item that they have ordered by mail/telephone but the Customer has sent an item where the colour, size, quality, etc. of that item differs from the original description.
- Non-receipt of merchandise – If a Cardholder orders goods by mail/telephone but they do not receive the item by the agreed date of receipt.
- Services not rendered – If the Cardholder has paid for a service and the Customer is unwilling/unable to provide that service by the agreed date.
- Incorrect currency – If the Cardholder signs a paper voucher for one currency but the Transaction is processed in another currency to his/her account.
- Accepting a Card with a violated or tampered signature stripe.
- Card was not present at the point of sale (POS) and cardholder is disputing the transaction - even despite an authorisation code being obtained for a transaction , due to lack of Cardholder authorisation or consent.
- Failure to respond to a Copy Request within a stipulated timeframe (copy attached as Appendix 1)
- Failure to properly disclose a limited return/cancellation policy at the time of a purchase or reservation.

Section 9 – iMerchantConnect

9.1 iMerchantConnect

www.iMerchantConnect.com

iMerchantConnect is an innovative online service offering you the opportunity to view your accounts online wherever and whenever you choose. iMerchantConnect is a completely free service and does not incur any fee's or charges.

9.2 Key Features of iMerchantConnect Service

Account Information

- View the date funds were last transferred to your account.
- View Retrieval Requests and Chargebacks.
- View your business profile.
- Information on troubleshooting and compliance issues.
- Restrict users to certain Merchant ID numbers (MID numbers) or groups of MID numbers on a log-in basis to allow flexible controls over users' access.
- See your Merchant Service Charges for the previous month's Statement.

Review Sales

- See your sales turnover by Card type for the current month.
- Confirm deposits.
- View batches and Transactions.
- View monthly statements for the previous 12 months.
- Analyse your turnover for the previous 12 months.
- Multiple-outlet Customers will appreciate the roll-up functions that allow them to see an aggregated view of their entire business.
- Account information available at your fingertips – no more calls to individual sites trying to trace Transaction information.
- Ability to search for specific transactions using the card search functionality

Section 10 – PCI DSS

The Payment Card Industry Data Security Standards (PCI DSS) is a set of requirements for enhancing payment account data security. These standards were developed by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International to facilitate industry-wide adoption of consistent data security measures on a global basis.

You, and any Third Party Vendors that you utilize, must comply with all applicable requirements of the PCI DSS, including Visa's Cardholder Information Security Program , MasterCard's Site Data Protection Program and the Discover Information Security & Compliance program. You must remain in compliance with these standards as they change.

For additional information please visit: **www.elavon.com/pci**

Section 11 – Exception Charges

Pricing for your Merchant Service Charge (MSC) is based on you processing your transactions in the most advantageous way, thus enabling a low rate on the majority of transactions. However, some types of transactions attract higher cost transactions. Exceptions fees were developed to be able to identify those specific transactions and charge a small additional fee to cover these higher costs.

The primary exception fees are

1) Downgrades: A downgrade takes place where the way in which the card is processed increases the cost of processing, for example key-entering details of a Chip&PIN Card, or sending transactions to Elavon late, which results in missing cut-off times with the Card Schemes. Thus in certain situations You can take action to avoid an Exception Charge.

2) International cards or Business & Personal Premium Cards: These are cards which carry higher costs and unfortunately no action taken by you can avoid an Exception Charge for these card types.

Below are some tips that may help you avoid incurring Exception Charges:

General Guidelines:

a. Upgrade to a chip & pin terminal if you have not already done so.
b. Obtain an electronic authorisation for each transaction.
c. Batch your Terminal at close of each business day.

Card Present Transactions

a. Use a chip capable terminal for all cardholder present transactions.
b. Insist on pin verification for Chip Card transactions.
c. Avoid hand keyed transactions.

Internet Transactions

Secure Internet Transactions will not attract Exception Charges.

Please remember: Not only are there cost implications of processing in a less secure way, but also this may leave You open to a higher risk of fraud and or chargebacks.

Section 12 – Other Useful Information

Retention of Documentation:
You must retain, in a safe and secure place, copies of your sales and Refund Transaction Receipts and also summary vouchers used, for at least two (2) years, in case there is any dispute regarding a Card Transaction. The Card Issuer may ask you to supply documentation for a particular Card transaction. This must usually be provided within fourteen (14) Business Days of the request, either in its original form or as a copy. In some exceptional circumstances, e.g. Card fraud, the Card Issuer will ask you to supply the documentation within 48 hours of the request. You must supply the documentation within this time when requested to do so. When destroying documentation after two (2) years, be sure to do so in a secure manner.

Advertising / Point of Sale Display:
If you wish to advertise in the press or other media to show that you accept Cards as a method of payment, the following rules apply:

- The Card Scheme logos have been registered as trademarks and must be used in accordance with instructions issued and available from the Card Schemes. If you wish to obtain further details regarding advertisements, please contact our Customer Service Team.
- The Card Scheme logos must not be featured in advertising in a manner where endorsement of the goods and/or services being offered by you, is given or implied.
- Card decals/stickers are provided to all Customers with Card Present business. These must be clearly displayed in your outlet(s).

Change of Bank Account Details:
If you change your nominated bank account, as defined in the Terms of Service, you must complete and return a new Direct Debit Mandate form. These can be found on our website at
www.elavon.com/acquiring/united-kingdom/collateral/index.aspx

Change of Ownership/Status/Name/Address:
In accordance with your Terms of Service if your business (or any of its outlets) changes ownership, status, products sold and/or services supplied, name or address, you should immediately inform our Customer Service Team and follow their instructions.

Broken or Faulty Imprinters:
If you have any problems with broken or faulty Imprinters, contact our Partner Company Paper Rolls on one of the below numbers:

From Ireland 00800 8438 0300
From UK 01698 843 866

Or visit **www.elavonconsumables.com to order new equipment.**

What to do if a Card is left at your premises:
Contact the Card Issuer immediately for further instructions. The telephone number is to be found on the back of the Card.

Section 13 – Glossary

Acquirer:
A financial institution which processes card transactions accepted at the Customer's premises as payment for goods and/or services.

Approval:
When a Transaction is approved it means that there are enough funds in the account and that the Card has not been reported lost/stolen at the time of the Transaction. Therefore, you must take additional steps to ensure the Transaction is genuine. Remember an Authorisation Code/Approval does NOT guarantee payment. Please refer to your Fraud Manual for further details.

AVS (Address Verification Service):
AVS is a cardholder verification tool designed to help reduce the risk of Transactions in Mail Order and/or telephone orders. Verification results help you to determine whether to accept a particular transaction.

Chip:
A microchip that is embedded in a Card that contains Cardholder data in an encrypted format.

Code 10:
Code 10 is a recognised code which has been designed to warn Authorisations centres when Customers are dealing with suspicious Transactions.

Declined:
When you get a declined response from the Authorisations centre or electronically through the Terminal this means that the Issuer cannot authorise that Transaction. In this case, the Cardholder will need to contact their Issuer to find out why, and use an alternative method of payment.

Imprinter:
A machine which takes an imprint of the Cardholder's Card onto a paper voucher.

IVR:
Interactive Voice Response or Phone Menu – a list of options upon calling our customer care numbers to best direct your call.

PAN key entry:
A service which may be provided at a Terminal where Card details embossed on a Card are keyed into the Terminal instead of the Terminal reading the Card's magnetic stripe.

Referral:
Routine security check on a Card, where response comes from the Issuer. In this case you will need to contact the Authorisations centre to obtain Approval.

Appendix 1 – Retrieval Request Form

Chargeback Department
PO Box 466
Brighton
BN50 9AW
United Kingdom
Phone: 0845 850 0195
Fax: 0845 6002465
Monday-Friday 9:00 a.m. to 5:00 p.m. GMT

A. MERCHANT
123 STREET
LONDON
E12

Copy Request

For prompt service, please return this cover letter with your rebuttal.

Following is a credit card charge from your business. Please locate the item and return it immediately.

Merchant Information	
Merchant Name:	
Merchant Number:	Ref No.:

Transaction Information	
Cardholder Account #:	Retrieval Amount:
Acquirer Reference #:	Original Transaction Amount:
Transaction Date:	Dynamic Currency Amount:
Transaction ID:	Ticket #:

Why Card Issuer Is Requesting Copy:

IMPORTANT REMINDER:

Please attach a legible copy of the white portion of the sales receipt to this form, and return it to the Chargeback Department immediately upon receipt of this request. If faxing, please send a clear and legible copy of the original sales receipt. To verify receipt or legibility of your response, please allow seventy-two hours before calling for status. Card Association regulations state that if an issuer initiates a non-receipt chargeback, the chargeback will be charged to your account, and cannot be reversed. It is extremely important that you respond immediately to meet all Card Association regulations. Items ruled illegible by the Card Associations are also subject to chargeback and association fines.