UK Operating Guide

Table of Contents

Section 1 – Introduction 3

Section 2 – Authorisation 4

Section 3 – Electronic Processing 7

Section 4 – Statements 9

Section 5 – Fraudulent Transactions 11

Section 6 – Back Up Procedures – Paper Processing 17

Section 7 – Chip and PIN – Contactless 19

Section 8 – Chargebacks 20

Section 9 – iMerchantConnect 22

Section 10 – PCI DSS 23

Section 11 – Exception Charges 24

Section 12 – Terminals 25

Section 13 – Authorisation and SCA 27

Section 14 – Transactions 30

Section 15 – Refunds 30

Section 16 – Services 32

Section 17 – Internet Transactions 39

Section 18 – DCC Transactions 41

Section 19 – Electronic Gift Cards 42

Section 20 – Purchase with Cashback 43

Section 21 – Customer's Representations for Cyber Security Tools 44

Section 22 – PCI Waiver Plan 45

Section 23 – Other Useful Information 46

Section 24 – Glossary 47

Appendix 1 – Retrieval Request Form 49

Appendix 2 – Solutions and PCI Waiver Plan 50

Appendix 3 – Unregulated Hire Terms 61

Appendix 4 – Goods 64

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 assureyou 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 24 – 'Glossary'), capitalised words and phrases used shall have the samemeaning 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. **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 Processing' – 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 your jurisdiction 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

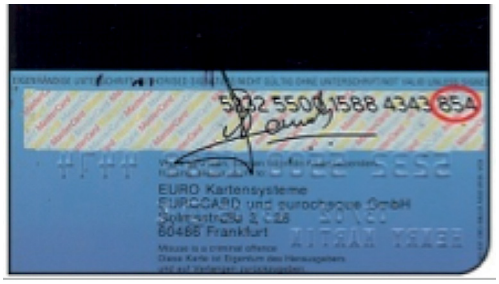
Watch out for:

- 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 Maintenance System Security

- 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

5.8 Third Party Processing

You must never process another person's Card Transactions. That's known as third party processing or transaction laundering and to do so would be a breach of the terms of your Agreement. Please report any person who approaches you to do so.

Section 6 – Back Up Procedures – Paper Processing

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, paper vouchers should be submitted to us for processing within three (3) Business Days from original transaction date.

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.

How to order Imprinters/Paper Vouchers

Imprinters and Paper Vouchers can be purchased from our partner Paper Rolls. They can be contacted directly on the telephone numbers below

From Ireland: 00800 8438 0300
From UK:: 01698 843 866

Paper vouchers can also be ordered by visiting this website: **www.elavonconsumables.com**

To Submit Paper Vouchers to Elavon for Processing

ADDRESS: **DATAPRO, PO BOX 466, Brighton BN50 9AW**

FAX: **0044 (0)1273 734 017**

EMAIL: **documents@elavon.com**

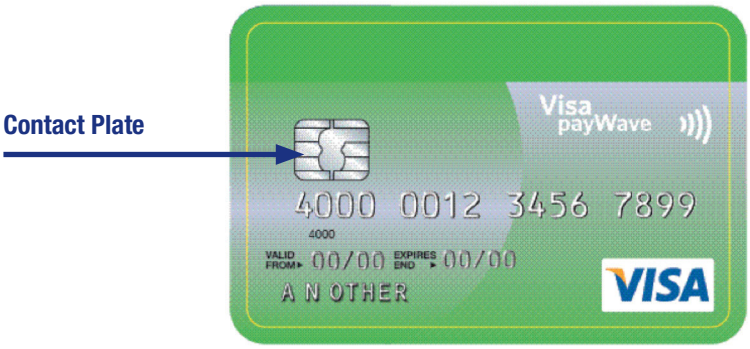
Section 7 – Chip and PIN – Contactless

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 calls 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 Customer 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's 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 – Terminals

1. Chip and PIN Technology.

1.1. You are responsible for ensuring that your Terminals, and your use of those Terminals are Chip and PIN Compliant.

1.2. You shall have sole and exclusive liability for fraudulent Transactions that occur but which, could have been prevented had you been Chip and PIN Compliant. Without limiting the foregoing, subject to the terms of the Agreement, liability for all failed or fraudulent Transactions carried out using C&P Cards will in any event rest with you, in any case, where you accept a C&P Card Transaction:

(i) using a Terminal or Third Party Terminal that does not incorporate Chip and PIN Technology;

(ii) using a Terminal, Card Reader or Third Party Terminal which incorporates Chip and PIN Technology but does not use the Chip and PIN functionality to accept the C&P Card Transaction

(iii) without using a PIN Pad.

2. Use and availability of PIN Pads

2.1. A Cardholder's Card information and PIN are confidential. You may not request or require a Cardholder to disclose his/her PIN at any point during payment. During the Transaction process, you must provide a reasonably secure area for Cardholders to enter their PIN into the PIN Pad. You shall cause a Terminal and PIN Pad device to be readily available at your locations for use by all Cardholders whenever C&P Cards are accepted. You shall take all reasonable steps to ensure that all Terminals and PIN Pads function with a minimum of error, in a reliable manner and in accordance with the standards established from time to time by Elavon and the Card Schemes.

2.2. Except where otherwise allowed by the Card Scheme Rules or the Laws, you shall use a Terminal to initiate every C&P Card Transaction and you shall require that either the Cardholder or you insert and/ or swipe the C&P Card through the Terminal. No C&P Card Transaction may be initiated unless the C&P Card is physically present.

2.3. You shall require that each Cardholder enter his/her PIN using a PIN Pad at the Terminal. Unless otherwise allowed by the Card Scheme Rules or the Laws, you cannot request a C&P Card Cardholder to sign a Transaction Receipt or other receipt, or require any other means of identification.

2.4. Subject to the Laws and the Card Scheme Rules, in the event of Chip Failure during a C&P Card Transaction, the Transaction may be completed as a magnetic-stripe-read Transaction but must be submitted for Authorisation, in accordance with the procedures detailed in the Operating Guide.

2.5. If you accept C&P Cards, no data referencing the Cardholder's PIN shall be printed on any Transaction Receipt.

3. Refunds

3.1. If permitted by the applicable Card Scheme, you may electronically process a Refund for a C&P Card Transaction but only if it is same customer named on the Transaction Receipt where the original C&P Card Sales Transaction was initiated. A Refund requires the following procedures:

3.1.1. the Card must be inserted and/or swiped through the Terminal;

3.1.2. the Cardholder must re-enter the PIN on the PIN Pad;

3.1.3. You must transmit the Authorisation Code and the exact amount (in the relevant currency) of the Transaction (or part) to be credited or refunded.

4. Manual Processing (or Back-Up Procedures)

4.1. If for any reason your Terminal ceases to function correctly or at all (e.g. it is unable to read the magnetic stripe on a Card), you will, with respect to Cards, follow the manual or other back-up processing procedures in the Operating Guide or other Terminal user guide, and shall otherwise follow any procedures specified by Elavon. Any manual Transaction Receipts must comply with the data requirements from time to time of the relevant Card Scheme.

5. Wireless Terminals

5.1. Limitations of Wireless Technology: If you use a Card Reader or other Wireless Terminal, you acknowledge and agree that due to the nature of wireless technology, certain limitations exist that may affect the performance, Coverage Area and reliability of wireless technology and wireless processing in relation to a Card Reader or other Wireless Terminal. In the event that your ability to process wireless Transactions is limited or prevented for any reason, you agree not to use the Wireless Terminal and instead, to process the Transaction using alternative means as set out in the Agreement.

5.2. Completing Unauthorised Transactions. If you choose to complete a Card Reader or other Wireless Terminal Transaction without an Authorisation Code or without SCA as required by the Operating Guide because wireless coverage is not available or otherwise (e.g. you store Transaction data in a Card Reader or other Wireless Terminal, provide the Cardholder with goods and/or services and subsequently request Authorisation of the Transaction), you do so entirely at your own risk.

Section 13 – Authorisation and SCA

(a) **Authorised Floor Limit.** Unless otherwise agreed by Elavon in writing, the Authorised Floor Limit for Sales Transactions shall be zero. You must not split the value of sales made to a Cardholder at any one time over more than one Transaction to avoid obtaining Authorisation.

(b) **Authorisation Code Required.** You must obtain an Authorisation Code before completing any Sales Transaction whether electronically through use of a Terminal or verbally by telephoning for an Authorisation Code in accordance with the Operating Guide.

(c) **Effect of Authorisation Code.** An Authorisation Code does not:

(i) Guarantee you payment for a Sales Transaction;

(ii) guarantee that a Sales Transaction will not be disputed later by the Cardholder or Issuer as any Sales Transaction is subject to Chargeback;

(iii) protect you in the event of a Chargeback regarding unauthorised Sales Transactions or disputes involving the quality of goods and/or services;

(iv) prevent us from recovering a Chargeback or other amount with respect to a Sales Transaction where permitted under the terms of this Agreement;

(even in each case, where "Code 10" procedures as provided in section 13(h), have been carried out).

(d) **Cancellation of Authorisation.** If you or the Cardholder decide not to proceed immediately with a Sales Transaction, you must cancel the corresponding Authorisation Request immediately.

(e) **No Authorisation.** If you do not make an Authorisation Request where required under this section, or if Authorisation is refused, you must not complete the Sales Transaction. Where the original Authorisation is refused, you must not resubmit a Sales Transaction for Authorisation. Should you do so, and you rely on any subsequent Authorisation, you will be liable (and if you are a Large Corporate or Large Charity (as defined in the Terms of Service) will indemnify us) in respect of any Chargeback, Fees and Adjustments or other losses in relation to such Sales Transaction.

(f) **Zero value Authorisations.** Authorisation Requests in order to validate a Card (usually for an amount between £0.01 and £1.00) are not permitted. You must process such requests as an Account Status Inquiry should you wish to validate a Card with no subsequent settlement, in accordance with the Card Scheme Rules.

(g) **Cardholder authority.** You must obtain authority for each Transaction to be debited to the Cardholder's account. Such authority shall be deemed given (unless the Card is reported lost, stolen or compromised):

(i) for a Transaction that is Card Present only when:

(aa) with respect to PIN Transactions, the Cardholder enters the PIN correctly into the Terminal, and promptly effects a successful PIN verification, or

(bb) you procure the Cardholder signature on the Transaction Receipt produced by the Terminal. The signed Transaction Receipt or printed Transaction record (following successful PIN verification) produced by the Terminal which shall constitute the Transaction Receipt, will in each case be evidence of the Cardholder's authorisation to debit the amount of the Transaction from the Cardholder's account.

(ii) for MO Transactions, by obtaining the signed written authority of the Cardholder and for TO Transactions, by retaining documentary evidence of the Cardholder's authority to debit his/her account for the Transaction amount.

(iii) for Internet Transactions, by obtaining the CVV2/CVC2 number from the Card.

(h) **Application of SCA.** SCA applies to all Sales Transactions, subject to section 13(k) and section 13(l) below. Unless otherwise agreed by Elavon in writing, you must:

(i) electronically request the application of SCA before completing any Sales Transaction, through the use of a Terminal or through the Service and Software (in the case of Internet Transactions);

(ii) enable and cooperate in the application of SCA to all Sales Transactions;

(iii) follow any instructions with regard to SCA received from an Issuer or Elavon, including instructions provided electronically through a Terminal or through the Service and Software (in the case of Internet Transactions). If an Issuer and Elavon give you incompatible instructions regarding the application of SCA to a Sales Transaction, you must give priority to the instructions of the Issuer.

(i) **SCA Decisions.** You must not:

(i) apply SCA on your own initiative if an Issuer or Elavon have not instructed you to do so;

(ii) split the value of sales made to a Cardholder at any one time over more than one Transaction or otherwise misrepresent the circumstances of a particular Transaction to avoid applying SCA.

(j) **No SCA.** If you do not request, enable or cooperate in the application of SCA where required under this section, or if SCA is unsuccessful, you must not complete the Sales Transaction. Should you do so, you will be liable (and if you are a Large Corporate or Large Charity (as defined in the Terms of Service) shall indemnify and hold us harmless) in respect of any Chargeback, Fees and Adjustments or other losses in relation to such Sales Transaction.

(k) **SCA Exemptions.** An Issuer or Elavon may decide not to apply SCA to certain Sales Transactions to the extent allowed by Laws and Card Scheme Rules, such as in the case of the following Sales Transactions:

(i) contactless Sales Transactions and Internet Transactions below thresholds specified in SCA RTS;

(ii) Sales Transactions at unattended Terminals for purposes specified in SCA RTS.

In such case you will be notified electronically through a Terminal or through the Service and Software (in the case of Internet Transactions).

(l) **SCA RTS Scope.** SCA does not apply to Sales Transactions that are outside the scope of SCA RTS, including:

(i) MO/TO Transactions;

(ii) Sales Transactions initiated by you.

(m) **Personalised Security Credentials.** A Cardholder's Personalised Security Credentials are confidential. You may not at any point during payment request or require a Cardholder to disclose his/her Personalised Security Credentials, capture or modify Personalised Security Credentials, capture or modify Authentication codes generated with the use of Personalised Security Credentials, or obscure or modify any information communicated through a Terminal or through the Service and Software by an Issuer or Elavon to a Cardholder in connection with the use of Personalised Security Credentials. During the Transaction process, if use of Personalised Security Credentials requires a Terminal, you must provide a reasonably secure area for Cardholders to use their Personalised Security Credentials through a Terminal.

(n) **Effect of SCA.** The application of SCA does not:

(i) guarantee customer payment for a Sales Transaction;

(ii) guarantee that a Sales Transaction will not be disputed later by the Cardholder or Issuer as any Sales Transaction is subject to Chargeback;

(iii) protect you in the event of a Chargeback regarding unauthorised Sales Transactions or disputes involving the quality of goods and/or services;

(iv) prevent us from recovering a Chargeback or other amount with respect to a Sales Transaction where permitted under the terms of this Agreement;

(even in each case, where "Code 10" procedures as provided in section 13(o) have been carried out).

(o) **"Code 10".** You must carry out a "Code 10" procedure (as applicable) in accordance with the Operating Guide.

(p) **Card Recovery.** You will use reasonable means to recover any Card in circumstances set out in the Operating Guide

(i) if you are advised by Elavon or instructed to do so by a Terminal, a Compatible Device, 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

(iv) with respect to MasterCard® branded Cards only, the Card does not have the "Twin Globes" hologram on the lower right-hand corner of the Card face.

(r) **No agency.** You must not suggest that you are acting on our behalf at any time, unless you are holding back or recovering a Card at our request.

(q) **Disputes with Cardholders.** Any dispute between you and a Cardholder relating to a Transaction will be settled between you and the Cardholder. Elavon shall bear no responsibility for such disputes.

Section 14 – Transactions

(a) **Transactions that are Card Present and Card Not Present.** You must use a Transaction Receipt to document each Transaction. A Transaction Receipt may be generated either electronically or manually and must include the following details:

(i) Card account number (and except where the only way to record a Card account number is in handwriting or by making an imprint or copy of the Card), such number being truncated so that all but the last four (4) digits of the Card account number on a Transaction Receipt are distinguished or suppressed. Truncated digits should be replaced with a fill character such as "x," "*," or "#," and not with blank spaces or numeric characters);

(ii) (ii) Customer's name and location;

(iii) Transaction amount (including applicable taxes) indicated in the Transaction currency such as GBP or £;

(iv) Transaction date;

(v) Authorisation Code;

(vi) Transaction type (e.g. purchase, credit);

(vii) for Card Present Transactions that are not PIN Transactions only, space for the Cardholder's signature;

(viii) for Card Present Transactions only, indication of who shall receive each copy of the Transaction Receipt (e.g., Customer's Copy, Elavon Copy, Cardholder Copy). The Cardholder copy of a Transaction Receipt must in particular, bear the wording "retain this copy for statement verification" or similar wording, which must as a minimum, appear in the language of the Transaction country;

(ix) for Card Present Transactions only, the terms and conditions of the sale, if restricted;

(x) for Card Present Transactions only, Customer's city and country;

(b) **Invalid Transaction Receipts.** A Transaction Receipt shall be invalid if it is not issued in accordance with the Agreement, Laws and Card Scheme Rules, including:

(i) the related Transaction is for any reason illegal or incomplete, or, has the result of making a Refund or credit with respect to gaming or gambling winnings, unspent gaming or gambling chips, or any other value useable for gaming or gambling;

(ii) where required, the signature on it is incompatible with that on the Card;

(iii) the copy of it that is presented to Elavon is incompatible with the copy provided to the Cardholder;

(iv) the Card has expired or has not yet become valid at the time of the Transaction;

(v) another such receipt has been issued for the same goods and/or services which are the subject of the Transaction (except in relation to sections 16(k), 16(l), or 16(m) below).

(c) **Delivery of Transaction Receipts.** For a Transaction that is Card Present, you will deliver a complete and legible copy of the Transaction Receipt (in either electronic (e.g. e-mail, text message (SMS) or fax) or paper (e.g., handwritten or Terminal-generated) format) to the Cardholder at the time of the Transaction. For a Transaction that is Card Not Present, this shall be done promptly but in any event, no later than seven (7) days following completion of the Transaction.

(d) **Higher Risk Additional Loading Transactions**

(i) The Higher Risk Additional Loading Fee will apply to Higher Risk Additional Loading Transactions.

(e) **Deferred Authorisation Transactions.**

(i) With Elavon's prior written consent, you may accept Deferred Authorisation Transactions for the certain Card Schemes. Please consult your relationship manager within Elavon for further details of which Card Schemes support this service.

(ii) The only Transactions that can be processed using this service are Card Present using Chip and PIN or Contactless.

(iii) You will be required to use a Supervisor Password to activate the Terminal's capability to accept Deferred Authorisation Transactions whilst it is in its offline function.

(iv) Only certain types of Transaction can be carried out as Deferred Authorisation Transactions and this may vary over time. Please consult your relationship manager within Elavon for further details on the scope of this service.

Section 15 – Refunds

(a) In order to evidence a Refund, you will issue a Refund Receipt, offering to give a copy to the Cardholder.

(b) In no event will you present a Refund that exceeds the amount of the original Sales Transaction. You will comply with applicable Laws when processing Refunds. You will only make a Refund to the same Card or the same Cardholder's account which was used for the original Sales Transaction. You must not make a Refund with cash where the original Sales Transaction was made using a Card, unless required by the Laws, nor accept cash or other compensation for making a Refund to a Card.

(c) The amount of each Refund represents a debt immediately due and payable by you to us irrespective of whether we make demand upon you for the value of any Refund. Elavon may debit Your Bank Account for the total amount of each Refund submitted to Elavon (less its Merchant Service Charges). If the value of Refunds is more than the value of Sales Transactions, the difference will be due from you to Elavon and we will debit the difference from Your Bank Account.

(d) Unless otherwise agreed, in no event will Elavon be obliged to process returns, refunds, or adjustments related to transactions not originally acquired by Elavon.

(e) Elavon may, in its sole discretion, refuse to accept any Refund. If we do refuse to accept a Refund, we will notify you (unless prohibited by the Laws) of the refusal and, if possible, the reasons for such a refusal.

Section 16 – Services

(a) (i) in relation to the purchase of gambling services only and in addition to the above requirements at section 14(a)(i-x), a Transaction Receipt must also include the following details:

(aa) Terminal number;

(bb) date of play; and

(cc) net amount of winnings or losses.

(ii) in relation to Internet Transactions only and in addition to the above requirements at section 14(a)(i)-(x), insofar as applicable, a Transaction Receipt must also include the following:

(aa) Cardholder address

(b) **Presentation of Transactions to Elavon.** Unless otherwise agreed with Elavon in writing:

(a) you shall, subject to sections 16(b)(b) of this Guide and section 26 of the TOS present all Transactions to Elavon within three (3) Business Days of the date of such Transaction , and in all events, within thirty (30) Business Days from such date for a MasterCard® Transaction and twenty-one (21) Business Days from such date for a Visa Transaction;

(b) MO/TO and Internet Transactions must not be presented until the relevant goods ordered by the Cardholder have been dispatched or arrangements made for services to be provided. Notwithstanding the foregoing: (aa) Visa MO/TO and Internet Transactions for goods may be presented before the dispatch of the goods or performance of the services, provided that within seven (7) days of presentation a written acknowledgement quoting the dispatch date is sent by you to the Cardholder, such dispatch date not to be later than twenty-eight (28) days from the date of receipt of the order, (bb) MasterCard® Card MO/TO and Internet Transactions, must not be presented until after the goods are dispatched or the services are performed unless, at the time of the Sales Transaction, the Cardholder agrees to a properly disclosed delayed delivery of the goods or services.

(c) **Mail Order and Telephone Order (MO/TO) Transactions.**

(a) You may not accept MO/TO Transactions without Elavon's prior written consent to do so. For the avoidance of doubt, consent will be deemed to have been given by Elavon where you have included your anticipated MO/TO Transactions within your Application and that Application has been accepted by Elavon.

(b) If Elavon provides the consent set out in section 16(c)(a), for each MO/TO Transaction, you must retain in an accessible place and produce on demand documentary proof of dispatch of goods or supply of services rendered, for not less than two (2) years from the Transaction date.

(c) If you do accept MO/TO Transactions without the consent set out in section 16(c)(a), then without prejudice to Elavon's other rights and remedies under the Agreement or at Law, you may have to pay a surcharge on each such MO/TO Transaction.

(d) **Internet Transactions.**

(a) You may not accept or present to Elavon Internet Transactions and/or Internet DCC Transactions without Elavon's prior written consent to do so. For the avoidance of doubt, consent will be deemed to have been given by Elavon where you have included your anticipated Internet Transactions within your Application and that Application has been accepted by Elavon

(b) If Elavon provides the consent set out in section 16(d)(a), you must comply with the provisions set out in Section 17 in respect of Internet Transactions.

(e) **DCC Transactions.** You may not accept DCC Transactions without Elavon's prior written consent to do so. For the avoidance of doubt, consent will be deemed to have been given by Elavon where your Schedule of Fees sets out our fees in relation to DCC Transactions. If Elavon provides the above consent, you must comply with the provisions set out in Section18 in respect of DCC Transactions.

(f) **Electronic Gift Cards.** You may not accept EGCs without Elavon's prior written consent to do so. For the avoidance of doubt, consent will be deemed to have been given by Elavon where your Schedule of Fees sets out our fees in relation to EGCs. If Elavon provides the above consent, you must comply with the provisions set out in Section 19 in respect of EGCs.

(g) **Recurring Sales Transactions.** You may not accept Recurring Sales Transactions without Elavon's prior written consent to do so. For the avoidance of doubt, consent will be deemed to have been given by Elavon where you have confirmed that you accept Recurring Sales Transactions within your Application and that Application has been accepted by Elavon. If Elavon provides written consent you must:

(i) obtain a Recurring Sales Transaction Authority from the Cardholder;

(ii) obtain Authorisation at the first debit;

(iii) notify the Cardholder (aa) that his Recurring Sales Transaction Authority is subject to cancellation by the Cardholder at any time; and (bb) of any change to the Sales Transaction details set out in the Recurring Sales Transaction Authority at least fourteen (14) days prior to the subsequent debit;

(iv) not complete any Recurring Sales Transaction after receiving: (aa) a cancellation notice from the Cardholder; (bb) a notice from Elavon that authority to accept Recurring Sales Transactions has been revoked; or (cc) a response that the Card is not to be honoured;

(v) retain the Recurring Sales Transaction Authority for a period of 18 months after the final payment that is made pursuant to it, and produce the Recurring Sales Transaction Authority to us on demand;

(vi) comply with any applicable Card Scheme Rules requiring registration of Recurring Sales Transactions or other applicable Transaction security requirements; and

(vii) acknowledge and accept that a Cardholder has the right to revoke a Recurring Sales Transaction at any time up to the end of the Business Day preceding the day agreed for debiting funds.

(h) **Multiple Transaction Receipts.** You will accept payment for goods and/or services in a single Sales Transaction Receipt unless: (aa) partial payment is entered on the Sales Transaction Receipt and the balance of the Sales Transaction amount is paid in cash or by cheque at the time of the Sales Transaction; or (bb) a Sales Transaction Receipt represents an advance deposit for a Sales Transaction completed in accordance with the Agreement and the Card Scheme Rules.

(i) **Deposits.** You may not accept any Card payment representing a deposit or partial payment for goods and/ or services to be delivered in the future without Elavon's prior written consent to do so. For the avoidance of doubt, consent will be deemed to have been given by Elavon where you have completed the 'deposits' section within your Application and that Application has been accepted by Elavon. If Elavon provides written consent, you must execute one Sales Transaction Receipt when accepting the deposit Sales Transaction and a second Sales Transaction Receipt upon accepting the balance of the Sales Transaction. You will note the words "deposit" or "balance" on the applicable Sales Transaction Receipt. You will not present the Sales Transactions labelled or otherwise attributable to the "balance" until the goods have been delivered to Cardholder or services fully performed.

(j) **Future Delivery.** You may not present any Sales Transactions to Elavon (whether by electronic means or otherwise) that relate to the sale of goods and/or services for future delivery unless you have obtained the prior written consent of Elavon to do so. For the avoidance of doubt, consent will be deemed to have been given by Elavon where you have completed the 'upfront payments' section within your Application and that Application has been accepted by Elavon. If Elavon provides written consent, you must maintain sufficient working capital to provide for the delivery of goods and/or services at the agreed future date; such working capital shall be independent of any credit or proceeds resulting from future delivery Sales Transactions.

(k) **Purchase with Cashback.** You may not provide Purchase with Cashback without the prior written consent of Elavon to do so. For the avoidance of doubt, consent will be deemed to have been given by Elavon where you have completed the 'cashback' section within your Application and that Application has been accepted by Elavon. If Elavon provides such consent, you must comply with the provisions set out in Section 20 in respect of Purchase with Cashback.

(l) **Other Transactions.** You must obtain Elavon's prior written consent for other Transaction types including, pre-Authorisations (assured reservations); foreign exchange (Bureau de Change) Transactions; and contactless Card Transactions.

(m) **Prohibited Transactions.** You will not present to Elavon, directly or indirectly, any Transaction not originating from a Transaction directly between you and a Cardholder, or any Transaction you know or reasonably suspect or should know or reasonably suspect to be illegal, fraudulent or not authorised by the Cardholder. You will not present any Transaction (i) representing the refinancing or transfer of an existing obligation of a Cardholder, or (ii) that arises from the dishonour of a Cardholder's personal cheque. In all events, you must give reasonable assistance to Elavon in the prevention and detection of financial crime at your locations.

(n) **Multi-Currency Conversion.**

(i) If you submit Transactions for which you have offered to the Cardholder the goods and/or services in a currency (**Transaction Currency**) that differs from your chosen settlement currency (**Settlement Currency**) (**Multi-Currency Conversion**), then, in addition to the other processing fees payable for a Transaction, Elavon shall apply a conversion rate calculated daily by Elavon for each Multi-Currency Conversion. For the purposes of PSD 2 and other equivalent regulations transposing PSD2 in each EU Member States, the conversion rate will be shown in the Reporting Tool.

(ii) For the avoidance of doubt, if the Transaction Currency and Settlement Currency are the same, no Multi- Currency Conversion shall be required and no conversion rate shall be applied to such Transaction.

(o) **Secured Pro**

(i) Subject to: (a) making and complying with the representations that appear in the Section 21; and (b) your payment of the Secured Pro Fees and compliance and/or acceptance of the matters covered in sections 6(q)(ii) to 6(q)(x), You shall be entitled to use the Cyber Security Tools.

(ii) Each time you avail of any scanning Cyber Security Tools (where applicable) you authorise us or our suppliers or providers to perform the scanning on the IP addresses you provide in relation to such scanning and you acknowledge and confirm that:

(a) it is your responsibility to identify the IP addresses and fully qualified domain names in scope for scanning;

(b) any IP addresses to be excluded from the scan scope have been segmented from the list of included IPs;

(c) the scope of IP addresses to be tested is accurate and correct to meet PCI DSS requirements and comprises all externally facing IP addresses that could impact the security of your cardholder data environment;

(d) if you require validation of scope you have advised us prior to commencement of any scanning;

(e) you have coordinated with and obtained any necessary consent from your internet service provider and/or hosting provider to permit scans to run, where applicable;

(f) you will ensure that our scanner IP addresses are white-listed through any active protection systems for the duration of the test to avoid any scan interference;

(g) your domain and IP addresses will grant access to our provided IPs;

(h) you have advised us of any load balancers in use;

(i) you have made any temporary configuration changes to your network devices as may be necessary to obtain a scan that accurately assesses your external security posture and will reapply your previous configuration as soon as the scan is complete;

(j) you have advised us of any legacy systems or unreliable operations that might not respond well to testing; and

(k) you have created a full back-up of all systems to be tested and know how to use those back-ups to recover and restore systems to normal operations.

(iii) In connection with your use of the Cyber Security Tools: you may provide us or our suppliers and providers with; we or our suppliers and providers may access; and/or a Cyber Security Tool may provide to us or our suppliers and providers: device information and status, location, application list and licence list; certain information about your use of a Cyber Security Tool including statistics relating to the use of the Cyber Security Tool, performance metrics relating to the Cyber Security Tool, and configuration settings, performance data, installed software; information about: applications, date, operating system, CPU information; if potential malware is running; system information; log data about your website's web traffic, including but not limited to signatures, request/response headers, source IP and time; the file/application list scanned; reporting of information of scan events; administrator access control for a device; any files or programs that are unknown or untrusted or identified as potential malware, including information on the actions taken by such files. The collected files could contain personal data that has been obtained by the file that has been identified as unknown, untrusted or potential malware without your permission. Such information may also be provided to our suppliers and providers, including Comodo Security Inc. ("Comodo"), who assist us with the provision of the Cyber Security Tools.

(iv) A Cyber Security Tool may provide containment services that isolate unknown programs. By default any unknown programs identified as potential malware are executed inside a containment sandbox and then automatically sent to Comodo for malware analysis. If a program is found by Comodo to be malicious it is then added to the Cyber Security Tool malware definitions list. If it found to be safe it is added to a safe program list. The next time the relevant Cyber Security Tool receives antivirus updates, it scans all the programs running inside the containment sandbox. If any program is found to be malicious, the containment sandbox isolates the program and moves it to the quarantine list. Safe programs are removed from containment and are no longer executed inside containment. If you wish you may request disabling of containment and/ or automatic submission of programs to Comodo.

(v) Your subscription may include the Web Security Gateway Cyber Security Tool, which is provided by Comodo. The Web Security Gateway is a service for websites and applications that combines a Web Application Firewall ("WAF") provisioned over a secure content delivery network ("CDN"). The CDN is a network of globally distributed servers to assist in the performance of websites and web applications by delivering content with use of the closest server to the user. Web traffic will be sent to Comodo's servers and inspected by Comodo, with the traffic routed based on geo-balancing. If you subscribed to the Web Security Gateway Cyber Security Tool, you authorise us to route your website's traffic via the Comodo CDN, to manage the website DNS, monitor for and/or block malicious activity and attacks against the relevant website etc. As part of the consideration of your use of the WAF, you may be required to (1) provide domain and SSL certificate information, (2) download and install software relating to the WAF, (3) reconfigure website settings, firewalls, antivirus solutions, and other IT security services that interfere with or prevent the WAF from operating correctly, and (4) continuously forward Subscriber Information. "Subscriber Information" means log data about your web traffic, including but not limited to, signatures, request/response headers, source IP, and time. Once you have completed the above installation requirements (if any), which shall be determined by us at our sole discretion, the Web Security Gateway will start analysing Subscriber Information. Services relating to the Web Security Gateway do not include any remediation assistance from us nor shall we be responsible for assisting you in correcting or eliminating any security flaw or vulnerability. Services relating to the Web Security Gateway do not, and are not intended to, fix, remedy, prevent, or eliminate vulnerabilities or other insecurities. Remedying any vulnerabilities or insecurities is solely your responsibility. You acknowledge and agree that it is your responsibility to monitor the expiry date of website certificates, ensuring their renewal prior to expiry, to ensure continued operation of the Web Security Gateway Cyber Security Tool and the relevant website.

(vi) We or our licensors or suppliers own all intellectual property in and to the Cyber Security Tools. The Cyber Security Tools are being licensed, not sold. The Cyber Security Tools contain material that is protected by intellectual property laws, including copyright, trade marks and trade secrets. All rights not expressly granted to you herein are reserved. You may not remove any copyright or other proprietary notice from any Cyber Security Tool. Certain Cyber Security Tools contain certain open source products and licences relating to them and what these are and where they can be found has been set out at in clause 6(e)(x).

(vii) Our total liability in relation to the Cyber Security Tools, whether to you or another party, howsoever arising shall not exceed in the aggregate an amount equal to the Secured Pro Fees paid by you during the twelve (12) months immediately preceding the first act or omission that formed the principal basis of the loss or claim being sought.

(viii) For the purposes of the Cyber Security Tools, the definitions of "We", "Us", "Our" and "Elavon" include Elavon's subcontractors including Sysxnet Limited a limited liability company incorporated under the laws of Ireland with company number 147176 and a registered office at 1st Floor, Block 71a, The Plaza, Park West Business Park, Dublin 12, Ireland.

(xi) You will not, and will not permit any third party to: use any Cyber Security Tool in a way that may infringe the privacy or intellectual property rights of a third party. You will not, and will not permit any third party to: use any Cyber Security Tool to distribute or transmit any file that contains malware or in any manner that is not lawful. You will not, and will not permit any third party to: export or re-export either directly or indirectly, any Cyber Security Tool to any country or entity under United States, United Kingdom or European Union restrictions or to any country or entity subject to applicable trade sanctions and you represent that you are not located in any such country. You have the necessary rights and licences to any files submitted to us for scanning. You also represent that your submission to us of any files will not violate any third-party rights to such files, including intellectual property rights and rights to privacy.

(x) The following third party or open source software may be included and is provided under other licences and/or has source available from other locations.

Framework/Software	Licence URL
OpenSSL	https://www.openssl.org/source/license.html
Zlib	https://www.zlib.net/zlib_license.html
SQLite	http://www.sqlite.org/copyright.html
QTCore v 4.8	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
FileHash.h	https://github.com/JoeKun/FileMD5Hash/blob/master/Library/FileHash.h
NSPR	https://github.com/servo/nspr/blob/master/LICENSE
Open LDAP	https://github.com/LMDB/lmdb/blob/mdb.master/libraries/liblmdb/LICENSE
LuaJIT	http://luajit.org/luajit.html
JSON	https://www.json.org/license.html
YAML::Syck	http://search.cpan.org/dist/YAML-Syck/lib/YAML/Syck.pm#COPYRIGHT
jQuery UI	https://github.com/jquery/jquery-ui/blob/master/LICENSE.txt
jQuery Bonsai	https://github.com/aexmachina/jquery-bonsai/blob/master/LICENSE.txt
jQuery Qubit	https://github.com/aexmachina/jquery-qubit/blob/master/LICENSE.txt
Chromium	https://chromium.googlesource.com/chromium/src/+/master/LICENSE
7za.dll	https://www.7-zip.org/license.txt
TOR	https://github.com/torproject/tor/blob/master/LICENSE
Oracle Java 7	http://www.oracle.com/technetwork/java/javase/terms/license/index.html
Apache Maven 3.3.1	http://www.apache.org/licenses/LICENSE-2.0
Mongo DB 3.0	https://www.mongodb.com/community/licensing
Apache Tomcat 8	http://tomcat.apache.org/legal.html
Nginx	http://nginx.org/LICENSE
WinExe	https://github.com/skalkoto/winexe/blob/master/COPYING
Spring Boot	https://github.com/spring-projects/spring-boot/blob/master/LICENSE.txt
Electron	https://github.com/electron/electron/blob/master/LICENSE
ReactJS	https://github.com/facebook/react/blob/master/LICENSE
Redux	https://github.com/reactjs/redux/blob/master/LICENSE.md
Python 3.6.5	https://docs.python.org/3/license.html
Nodejs	https://raw.githubusercontent.com/nodejs/node/master/LICENSE
Scapy	https://github.com/secdev/scapy/blob/master/LICENSE
Npcap	https://github.com/nmap/npcap/blob/master/LICENSE
Luhn	https://github.com/mmcloughlin/luhn/blob/master/LICENSE
Requests	https://github.com/requests/requests/blob/master/LICENSE
PyInstaller	https://github.com/pyinstaller/pyinstaller/blob/develop/COPYING.txt

(q) **High Risk/ Cost Additional Loading Transactions**

(i) The High Risk Additional Loading Fee will apply to High Risk Cost Additional Loading Transactions. High Risk Loading Transactions can only be carried out if the Card involved is MasterCard, Maestro or Visa.

Section 17 – Internet Transactions

1. Encryption

You may process Internet Transactions only if they have been encrypted by a Third Party Vendor acceptable to Elavon. Encryption is not a guarantee of payment and shall not waive any provision of the Agreement or otherwise validate a fraudulent Transaction.

2. Internet Security

You must (via a Third Party Vendor) utilise, or implement yourself, an internet payments service approved by Elavon in advance which adheres to minimum security measures and technology requirements identified by Elavon from time to time including, compliance with the PCI DSS. For Internet Transactions, you will be responsible for (i) maintaining the integrity of data received, held, maintained, or sent across the internet or other communication channel; (ii) managing the telecommunications link; and (iii) payment of all power and telecommunication costs. You will ensure that all Transactions are transmitted (where applicable) using the protocol approved by Elavon from time to time to procure the secure transmission of data provided by the Cardholder in ordering goods and/or services and effecting payment over the internet. You will provide capability for secure sockets layer encryption to the minimum standard from time to time (currently 128 bit), and may also be required by Elavon to support encryption requirements in respect of the transmission of information over the internet via a virtual private network ("VPN") supporting 3DES (1028 bit) encryption.

3. Online Authentication Solutions

You agree to implement and promptly update to the newest available versions, as designated by Issuers or Card Schemes (as applicable) from time to time, the Online Authentication Solutions, including by participating in the 3D Secure™ system, and to acquire the right to use or access Online Authentication Solution Plugins, including the MPI software, by:

(a) agreement with a seller of Online Authentication Solution Plugins, including MPI software, that is approved by the Card Schemes or Issuers (as appropriate); or

(b) having Elavon host the Online Authentication Solution Plugins, including MPI software, or such other merchant plug-in software or hardware product designated by Elavon from time to time, on your behalf, and on terms notified to you by Elavon; or

(c) procuring for your own use a customer plug-in software or hardware product of equivalent functionality to the Online Authentication Solution Plugin, including MPI software, subject to the prior written consent of Elavon.

4. Unauthorised Access

Whilst Elavon will take reasonable precautions in relation to use and access to the Service and Software, you hereby accept all risk of information or instructions being given by an unauthorised person and the possibility of hacking, cracking, viruses and any and all manner of unauthorised access, use, activity or purpose which may occur on or in relation to the Service and Software.

5. Website

Your website must:

(a) contain all of the following information:

(i) a complete description of the goods and/or services offered;

(ii) returned goods and refund policy;

(iii) customer service contacts, including electronic mail address and/or telephone number;

(iv) the Customer's name and/or any trading name (prominently displayed) and the complete address of the permanent establishment of your business on either the checkout screen (which displays the total purchase amount) or within the sequence of web pages presented to the Cardholder during the check- out process;

(v) Transaction currency;

(vi) export or legal restrictions, if known;

(vii) delivery policy;

(viii) Customer's data privacy policy;

(ix) your method of Transaction security and policy for transmission of Card details; and

(x) display of Card Schemes' marks;

(b) prominently identify the Customer's name as being both the Customer and as being the name that will appear on the Cardholder statement; and

(c) display the Customer's name information referred to in this paragraph 5 as prominently as any other information depicted on your website, other than images of the products or services being offered for sale.

6. Option to Cancel Payment

Your website will clearly inform the Cardholder that he/she is committing to payment before he/she selects the "pay now" or equivalent button/screen and will provide the Cardholder an unambiguous option to cancel the payment instruction at this point.

7. Cardholder Complaints

Elavon may investigate any complaint received from a Cardholder about the content of your website and shall be entitled to require you to amend and/or clarify the terms and conditions of sale within a period of thirty (30) days from the receipt of such complaint. [Elavon may charge a fee for doing so.]

8. Recurring Transaction Payments

If you offer recurring Transaction payments on your website you must: (aa) offer an online cancellation facility to Cardholders; and (bb) notify Cardholders at the outset that subsequent charges will be debited from their Card accounts.

Section 18 – DCC Transactions

1. The default currency of a Transaction must be the local currency of the Cardholder. The Customer must give to Cardholders, in clear terms, disclosing all charges, the choice of whether to proceed with the DCC Transaction in the Customer's local currency or the currency in which the Card has been issued (the "**Payment Currency**"), subject always to the chosen currency being a currency approved by Elavon (as communicated by Elavon to the Customer from time to time) (the "**Currency Payment Choice**"). The Customer must inform the Cardholder that selecting a DCC Transaction is optional and must not use inaccurate or misleading statements that could lead the Cardholder to select a DCC Transaction.

2. The Customer must disclose and make available to the Cardholder the following information prior to the Cardholder choosing to proceed with a DCC Transaction:

   (a) the Transaction amount in the local currency of the Customer;

   (b) the Transaction amount in the Cardholder's billing currency;

   (c) the exchange rate to be used and the source of the exchange rate; and

   (d) details of all charges, mark-up or commission to be applied. The total currency conversion charges shall be presented according to the applicable law – especially to the Regulation 2019/518 (within the scope of its applicability to a particular Transaction).

3. For every DCC Transaction using a Terminal, Customer shall ensure that it issues a document informing the Cardholder of the Currency Payment Choice and (except where Chip & PIN procedures are used) shall obtain the Cardholder's signature on this document.

4. For all DCC Transactions which are not Terminal DCC Transactions, the Customer shall obtain the Cardholder's prior consent to such DCC Transactions which must be in a form that clearly evidences that the Cardholder's express and final consent has been given in relation to the Currency Payment Choice. For Internet Transactions, this can be in the form of an email from the Cardholder or an "I agree" option on Customer's website which can be recorded and provided in the event of a dispute or Chargeback. For MO/TO Transactions, the requirements of section 16(g)(ii) on Cardholder authority apply in respect of DCC Transactions which are not effected with a Terminal.

5. Customer may not convert any DCC Transaction from the currency selected by Cardholder, into an amount in any other currency after the Transaction has been completed by the Cardholder.

6. As further detailed in paragraph 2, if the Cardholder elects to proceed with the Transaction in the Payment Currency, you must disclose to the Cardholder all your charges as well as the exchange rate to be used for converting the Transaction from the Cardholder's local currency into the Payment Currency prior to the Transaction being completed.

7. If the Cardholder elects to proceed with a DCC Transaction, the Transaction Receipt or invoice generated must contain:

   (a) the Transaction amount in the local currency of the Customer;

   (b) the Transaction amount in the Cardholders' billing currency;

   (c) the exchange rate used;

   (d) details of all charges, mark-up or commission applied and with respect to this the total currency conversion charges The total currency conversion charges shall be presented according to the applicable law – especially to the Regulation 2019/518 (within the scope of its applicability to a particular Transaction).

   (e) a statement that the Cardholder was given a choice and chose their billing currency. The statement must be in English, unless available in the Cardholder's local language.

8. Refunds (or credits) relating to DCC Transactions must be processed in the selected currency of the original DCC Transaction.

Section 19 – Electronic Gift Cards

1. Service

Elavon will provide electronic processing services of EGC Transactions (except where these are lost or stolen) and facilitate:

(a) electronic confirmation that the Cardholder activating the EGC Transaction through the Customer has an active account on the relevant processing system which is credited with sufficient funds to meet the cost of the Transaction; and

(b) debiting of the Cardholder's account with the value of the purchase and the crediting of the Cardholder's account if value is added to the EGC;

(c) maintenance of an accessible electronic record of an EGC Transaction for the lifetime of an EGC with a balance and for a period of sixty (60) days after the balance of the EGC Card has fully depleted.

2. Merchant Responsibilities

You shall:

(a) maintain all Transaction Receipts and any other receipts as required by the Laws, the EGC Rules and these TOS;

(b) maintain sufficient back-up information and data whether in paper or electronic form with respect to EGCs previously sold, to reconstruct any loss of information or data due to any malfunction of Customer's systems.

(c) in a timely manner when required by Elavon and/or Elavon's approved provider(s), execute all such agreements and do all such acts or things to enable Elavon to provide EGC processing services to Customer, including, entering into additional agreements for the supply of EGCs, for stationary and other related materials and for promptly settling accounts for such supply; and

(d) only use materials (including stationary and marketing materials) to enable the acceptance and processing of EGCs supplied by Elavon or Elavon's designated provider.

3. System Downtime

Customer shall not process EGC Transactions if the EGC processing system is down and is unable to verify the validity of an EGC and any available balance.

Section 20 – Purchase with Cashback

When providing Purchase with Cashback, you shall:

(a) only provide such facility in relation to Debit Card Sales Transactions where the Cardholder receives goods and/or services in addition to cash and only on Terminals approved for such use by Elavon;

(b) transmit in the Purchase with Cashback Sales Transaction message, the amount of cash given to the Cardholder (if permitted by Elavon's systems and/or the relevant Card Scheme);

(c) where a request for Authorisation of a Purchase with Cashback is refused solely because the cash requested exceeds the Debit Card Issuer's limit for cash withdrawals, inform the Cardholder of the reason for the refusal and that a new Sales Transaction in the amount of the purchase alone might be approved;

(d) not, where the amount of cash available to a Cardholder in a Purchase with Cashback Sales Transaction is limited by the relevant Card Scheme or Issuer, carry out a Purchase with Cashback Sales Transaction in excess of such limit, as notified to you from time to time;

(e) (e) not offer Purchase with Cashback in respect of Sales Transactions carried out under section 12(4).

Section 21 – Customer's representations for cyber security tools

You acknowledge and confirm that on and from the Commencement Date:

1. You will not, and will not permit any third party to: use any Cyber Security Tool for infringe the privacy or intellectual property rights of a third party;

2. You will not, and will not permit any third party to: use any Cyber Security Tool to distribute or transmit any file that contains malware or in any manner that is not lawful;

3. You will not, and will not permit any third party to: export or re-export either directly or indirectly, any Cyber Security Tool to any country or entity under United States, United Kingdom or European Union restrictions or to any country or entity subject to applicable trade sanctions and you represent that you are not located in any such country; and

4. You have the necessary rights and licences to any files submitted to us for scanning. You also represent that your submission to us of any files will not violate any third-party rights to such files, including intellectual property rights and rights to privacy.

Section 22 – PCI Waiver Plan

Subject to the terms of Schedule 2 of the TOS, you shall be entitled to receive the benefit of the waivers set out under the PCI Waiver Plan if you:

(a) meet the eligibility criteria specified in Schedule 2 of the TOS (including that you are classified as either a PCI Level 3 or Level 4 Customer and maintain such classification); and

(b) subscribe to one of the Solutions (as further described in Schedule 2 of the TOS)

Section 23 – 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 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 24 – 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.

B2B:
means business-to-business.

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.

Consumer Card:
means a Card issued to a natural person in his/her personal capacity.

Cyber Security Tools:
means the cyber security software or service subscribed to and provided in relation to the Programme as licensed pursuant to these terms and conditions;

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.

Higher Risk Additional Loading Transactions:
means the following Transactions:

(a) a Card Present not using Chip and PIN or Contactless e.g. swiping magnetic stripe, card holder signature;

(b) a Card Not Present not secured by 3D Secure ™ Transaction, occurring when the Customer accepts payment when Card Not Present and 3D Secure™ is not used e.g. 3DS not effective, telephone order, mail order;

(c) keying Card number into any device or data unknown;

(d) a delayed file submission Transaction, occurring when the Customer submits clearing file to Elavon 2 days or more (based on a 7 day week including Sundays) after the Card was accepted by the Customer.

Elavon reserves the right to reference Visa/Mastercard assessment of the above conditions being present or not present if required in applying the Higher Risk Loading

High Risk Additional Loading Transactions Fee:
means the high risk/ cost additional loading fee as set out in the Schedule of Fees.

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.

Non - EEA Country:
means a country which is not a member of the European Economic Area.

PAN: means the Primary Account Number of a Card.

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.

Programme:
means the proactive data security service you subscribed to, as offered by Elavon, including the provision of any relevant Cyber Security Tools.

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.

Secured Pro Fees:
means the fees for the Cyber Security Tools as identified in the Schedule of Fees.

Virtual Card:
means a digital Commercial Card, including a B2B virtual card.

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:

WHY CARD ISSUER IS REQUESTING COPY:

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.

Appendix 2. Solutions and PCI Waiver Plan

1. Definitions and Interpretation

1.1 In this Appendix 2 the following definitions shall have the meaning set out below. Any capitalized terms not defined below shall have the meaning given to them in the Glossary.

"**Device**" has the following meaning, which shall depend on the Solution you have subscribed to:

(i) for the purposes of the Secured Pro, the "**Device**" means any computer, laptop, mobile device, tablet or other computing system running on an operating system which is listed on the Website in the product information section relating to that Solution; and

(ii) for the purposes of Secured Encrypt, the "Device" means each Terminal (excluding always Third Party Terminals) which is Secured Encrypt enabled and provided under your Agreement, and in each case, references to "**Devices**" shall be construed accordingly.

"**Initial Subscription Period**" means in relation to either Secured Pro or Secured Encrypt, a period of twelve (12) months beginning on the date we accept and confirm your pricing for that particular Solution in your Schedule of Fees.

"**PCI Non-Compliance Fee**" has the meaning given to it in paragraph 11.3 of this Appendix 2. "Renewal Period" has the meaning given to it in paragraph 5.1 of this Appendix 2.

"**Secured PCI**" means the product available to PCI Level 3 or Level 4 Customers, which includes the following services:

(i) access to an online certification portal with Elavon's approved third party provider of PCI DSS;

(ii) specialist assistance in self-validation and maintenance of self-reported compliance;

(iii) access to downloadable Attestation of Compliance (for the purposes of PCI DSS) and certification of compliance documentation; and

(iv) the ability to run required quarterly scans performed by ASV at no additional cost through Elavon's approved third party provider of PCI DSS for merchants who require such scans to complete PCI compliance validation

"**Secured Pro**" means the product available to PCI Level 3 or Level 4 Customers provided by us or our third party representatives through or via the Website, over the telephone, by email, live chat or otherwise in connection with the Website, as more particularly described in Annex B of this Appendix 2 below and comprising of the following Services and/or Software:

(i) access to an online certification portal with Elavon's approved third party provider of PCI DSS;

(ii) outbound phone call from a PCI specialist;

(iii) management of PCI compliance validation over the phone;

(iv) access to downloadable Attestation of Compliance (for the purposes of PCI DSS) and certification of compliance documentation;

(v) ability to run required quarterly scans performed by an ASV scans at no additional cost through Elavon's approved third party provider of PCI DSS for merchants who require such scans to complete PCI compliance validation;

(vi) remote installation of relevant security tools as listed in Annex B of Appendix 2;

(vii) outbound call when remediation is needed as indicated as a result of a scan performed by an ASV; and

(viii) access to security tools as listed in Annex B of Appendix 2 below: network perimeter scan, device security scan, cardholder data discovery scan, antivirus license, POS application discovery scan.

"**Secured Encrypt**" means the product available to PCI Level 3 or 4 Customers and provided by us or our third party representatives through or via the Website, over the telephone, by email, live chat or otherwise in connection with the Website, and comprising of the following Services and Software:

(i) access to an online certification portal with Elavon's approved third party provider of PCI DSS;

(ii) outbound phone call from a PCI specialist;

(iii) management of PCI compliance validation over the phone; and

(iv) access to downloadable Attestation of Compliance (for the purposes of PCI DSS) and certification of compliance documentation.

"**Service**" means the services delivered under a particular Solution.

"**Software**" means software intended to be installed on a Device and shall include any Updates. "Solution" means one of the following: (i) Secured PCI; (ii) Secured Pro; or (iii) Secured Encrypt (as applicable).

"**Subscription Period**" means with respect to the relevant Solution subscribed to, the Initial Subscription Period together with all Renewal Periods.

"**Update**" means content or code we deploy to update the Solution (in whole or part) including revisions, additions, replacements, new releases or versions of Software and any available update provided by us from time to time in connection with the Solution.

"**Website**" means https://elavonsecuritymanager.com.

PCI Waiver Plan

2. Indemnity Waiver

2.1 Subject to the terms of this Appendix 2, a PCI Level 3 or Level 4 Customer who subscribes to a Solution may benefit from certain waivers from Elavon of Elavon's rights under this Agreement regarding indemnification by the Customer as follows (each of the following paragraphs 2.1 (i) – (iv) (inclusive) an "Indemnification Item")

2.1.1 certain fines imposed on Elavon by the Card Schemes arising directly from a Data Breach;

2.1.2 any Audit Costs incurred by Elavon in investigating any Data Breach (or where the Customer is obliged by this Agreement and/or the Card Scheme Rules to arrange a certified third party to carry out such Security Audit;

2.1.3 following a Data Breach Elavon shall waive any rights it has against the Customer under this Agreement to recover those investigation costs (if they fall due to be paid by Elavon) provided always that the third party is approved by the involved Card Scheme for the purpose of conducting such a Security Audit;

2.1.4 any fees Elavon is obliged to pay to Issuers to replace any Cards issued by Visa or MasterCard, which such Issuers must cancel following a Data Breach, provided always that such waiver shall only be available if you use Elavon's approved third party of PCI DSS assessment services pursuant to this Agreement.

3. Limitations

3.1 There shall be a maximum cap on the Customer's right to enjoy a waiver pursuant to this Schedule for each Data Breach depending on the Customer's PCI DSS compliance status according to Elavon's records, such that Elavon gives no waiver in relation to, and the Merchant shall be liable for any amounts over, the caps set out below. These caps shall be as follows:

3.1.1 any Customer who is certified as PCI DSS compliant by Elavon's approved third party provider of PCI DSS assessment services from time to time and is paying the applicable Fee relating to that MID for the Solution - £60,000 per Data Breach;

3.1.2 any Customer who is certified as PCI DSS compliant through a third party who is not Elavon's approved third party provider of PCI DSS assessment services from time to time and is paying the applicable Fee relating to that MID for the Solution – £30,000 per Data Breach;

3.1.3 any Customer who has not notified Elavon of its compliance status (deemed by Elavon to be non-compliant) (but has paid the applicable Fee relating to that MID for the Solution) – £6,000 per Data Breach.

Elavon reserves the right to amend the foregoing caps from time to time on notice to the Customer.

4. Eligibility

4.1 In order to be eligible for the waiver under the PCI Waiver Plan, the Customer must:

4.1.1 subscribe to a Solution in accordance with this Appendix 2;

4.1.2 be either a PCI Level 3 or Level 4 Customer;

4.1.3 within seven (7) days of its discovery, advise Elavon in writing of any failure of security within its business or its card acceptance systems that gives rise to or could give rise to a Data Breach;

4.1.4 comply with PCI DSS at the time of the Data Breach;

4.1.5 retain business records, logs and electronic evidence relating to a Data Breach;

4.1.6 provide audit reports of the Customer's computer systems to identify the source of the Data Breach or allow Elavon to conduct such a Security Audit;

4.1.7 co-operate with Elavon and the involved Card Scheme in all investigations relating to any Data Breach; and

4.1.8 have paid all Fees due and payable to Elavon for the Solution.

5. Ineligibility

5.1 If the Customer fails to comply with the steps set out in paragraph 4 of this Appendix 2, the waiver under the PCI Waiver Plan shall not be available and Elavon (and/or any party with rights of subrogation such as Elavon's insurers and/or underwriters) shall reserve the right to recover from the Customer all amounts which it would otherwise be able to claim under this Agreement including without limitation any fines assessed by the Card Scheme against Elavon and Audit Costs for which the Customer is liable.

5.2 In addition to the foregoing the Customer shall have no right to enjoy a waiver pursuant to this Appendix 2 if any of the following circumstances arise:

5.2.1 the Data Breach arises prior to the payment of the Fees for the Solution by the Customer;

5.2.2 the Data Breach arises out of any wilful default, or criminal act or omission of the Customer;

5.2.3 this Agreement is terminated (for any reason); or

5.2.4 the Customer's claim under this Appendix 2 does not relate to an Indemnification Item or is otherwise a Customer obligation under the Agreement governing the services rendered by Elavon.

6. Withdrawal or Suspension

6.1 Without prejudice to the accrued rights and liabilities of the Customer, the Customer further acknowledges that the PCI Waiver Plan may be withdrawn or suspended by Elavon on reasonable written notice.

7. Solutions

7.1 The terms of this Appendix 2 shall apply to your subscription of your Solution. For the avoidance of doubt, the terms of this Appendix 2 are intended to supplement and be read in conjunction with the rest of your Agreement. In addition, depending on the Solution you have subscribed to, the following terms shall also apply where:

7.1.1 you subscribe for Secured Pro, the licence terms at Part A of Annex A and the "Set-up, Description and Technical Details" at Annex B shall apply; and

7.1.2 you subscribe for Secured Encrypt, the licence terms at Part B of Annex A shall apply.

8. Exclusion of Liability

8.1 We do not warrant that the operation of Secured Encrypt or Secured Pro will be uninterrupted or error free, that Secured Encrypt or Secured Pro will work properly on any given Device or with any particular configuration of hardware and/or software, that Secured Encrypt or Secured Pro will provide complete protection for the integrity of any Device or against all possible threats, or that Secured Encrypt or Secured Pro will meet your requirements. We make no warranty as to the results that may be obtained from the use of Secured Encrypt or Secured Pro or as to the accuracy or reliability of any information obtained through Secured Encrypt or Secured Pro. No recommendation or information, whether oral or written, obtained by you from us or through or in connection with Secured Encrypt or Secured Pro shall create any warranty not contained herein. We disclaim any liability (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise howsoever arising) that may arise as a result of unused or incorrectly used recommendations provided by us or improper installation or removal of software or amendment or deletion of data. We shall have no liability (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise howsoever arising) for any damage caused by the implementation of or arising from any errors or omissions in any information, recommendation or script provided in connection with Secured Encrypt or Secured Pro or any actions taken by you at our recommendation.

8.2 You acknowledge and agree that any material, update, patch and/or data downloaded, installed, amended, deleted or otherwise used in connection with Secured Encrypt or Secured Pro is at your sole discretion and risk and that you will be solely responsible for: the results obtained from the use of either Secured Encrypt/ Secured Pro; for any conclusions drawn from such use; any damage to your Devices or any loss of data that results from such downloading or installation of that Solution.

8.3 You acknowledge that we may rely upon information provided by you in order to provide you with a Solution and accordingly you agree that we shall not be liable to you (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise howsoever arising) in any way to the extent such liability arises from the material inaccuracy of any such information or any material failure by you to provide information reasonably requested by us in relation to a Solution.

8.4 Nothing in this Appendix 2 shall exclude or limit any liability that cannot, as a matter of law, be limited or excluded.

9. Your Subscription

9.1 At the end of any Initial Subscription Period, your subscription for the Secured Encrypt or Secured Pro will automatically extend for an additional twelve (12) month period (each a "Renewal Period") at the end of the Initial Subscription Period or any Renewal Period (as applicable), unless you cancel your subscription by giving us notice (in accordance with the requirements of your Agreement) at least one (1) month before the end of the Initial Subscription Period or any Renewal Period (as applicable).

9.2 You may also cancel your subscription by giving notice at any time during the Subscription Period and any such cancellation will take effect at the end of the Initial Subscription Period or Renewal Period (as applicable) and will result in your subscription not being extended. You will remain liable for any Fees due in relation to the remainder of your Subscription Period and will retain access to your Solution until the end of the then-current Subscription Period.

9.3 Should we terminate your Agreement prior to the end of any Subscription Period for convenience, as set out in paragraph 10 of this Appendix 2 below, you shall only be liable for any Fees due in relation to the supply of the Solution up to and including the date of such termination.

10. Termination by Elavon

10.1 Without prejudice to any other rights and remedies set out in your Agreement, the Card Scheme Rules or at Law, we may and at our convenience:

10.1.1 At any time without cause during the Initial Subscription Period or any Renewal Period terminate your subscription to the Secured Encrypt or Secured Pro, subject to giving you two (2) months prior written notice; and

10.1.2 Suspend or terminate any part of our obligations for any Solution, with immediate effect, in the event of a material breach of this Appendix 2, and, where any such breach is capable of remedy, we have first provided you with written notice of the alleged breach and such breach remains un-remedied for a period of thirty (30) days following receipt of the written notice by you.

10.1.3 For the avoidance of doubt, both Parties' rights and conditions to terminate your Agreement also apply to the terms of this Appendix 2 for any Solution. Notwithstanding the foregoing, the Parties hereby acknowledge that termination of the terms for any Solution shall not result in the automatic termination of your Agreement, and that your Agreement can only be terminated in accordance with the terms set out in your Agreement.

11. Payment of Fees

11.1 In consideration for the provision of the Solution you will pay us the relevant Fee for the Solution by direct debit or by other payment method, as set out in your Schedule of Fees. The Fees are payable per MID, per month including the month in which your Initial Subscription Period commences, no matter when in such month it commences, but not the month in which your then current Subscription Period (whether it is your Initial Subscription Period or Renewal Period, as applicable) ends.

11.2 We will collect the Fees from you, in arrears, as per the terms of your Agreement.

11.3 PCI Non-Compliance Fee

11.3.1 The PCI Non-Compliance Fee is set out in your Schedule of Fees. You will be charged the PCI Non-Compliance Fee:

11.3.1.1 If you are a PCI Level 3 or Level 4 Customer that subscribes to Secured PCI;

11.3.1.2 If you do not certify your compliance with PCI DSS in accordance with paragraph 7(c)(ii) of this Appendix 2 within 90 days of completion of your boarding to Secured PCI. You will also be charged the PCI Non-Compliance Fee on a monthly basis thereafter, until you certify your compliance with PCI DSS in accordance with paragraph 11.3.2 of this Appendix 2; or

11.3.1.3 In the event you do not provide a renewed PCI DSS certification to Elavon in accordance with paragraph 11.3.2 of this Appendix 2. In this case, the PCI Non-Compliance Fee shall become payable again 30 days after the first anniversary of the last PCI DSS certification date you provided to Elavon.

11.3.2 The PCI Non-Compliance Fee will cease to become payable on Elavon's receipt of your PCI DSS certification. You should report your compliance with PCI DSS by providing details of your PCI DSS certification through the online portal available via your Secured PCI on the Website, or as otherwise advised by Elavon.

11.3.3 If a valid PCI DSS certification date is updated by the 25th of a given month in accordance with paragraph 11.3.2 of this Appendix 2, the PCI Non-Compliance Fee will not accrue for that month. If it is uploaded after the 25th of a given month, you will be liable for the PCI Non-Compliance Fee for that month.

11.4 We may from time to time vary the Fees and charges for the Solution and/or introduce new additional charges in accordance with your Agreement.

Annex A to Appendix 2

Licence Terms

1. Secured Pro Licence Terms

1.1. Subject to the terms of this Appendix 2, we, grant you a non-assignable, non-exclusive, revocable, limited and non-transferable licence to use the Solution during the Subscription Period.

1.2. You may use the Solution on up to 2 (two) Devices or up to 2 (two) IP addresses (as applicable, as specified in Annex B) for each licence purchased as specified in your Schedule of Fees under "Quantity" (save for the Antivirus Protection, as set out in Annex B, which is limited to 1 Device).

1.3. You will not, and will not permit any third party to:

1.3.1. Use any licence or other authorisation number provided by us in connection with the Solution on more than the number of Devices or against more than the number of IP addresses specified in this Appendix 2;

1.3.2. Disclose any licence or authorisation number for the Solution to any party other than to us or our authorised representatives;

1.3.3. Circumvent or attempt to circumvent controls on the installation or use of the Solution;

1.3.4. Copy, modify, change, alter, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Solution in any form or media or by any means nor attempt to do any such thing;

1.3.5. Reverse compile, disassemble, translate, reconstruct, transform, extract, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software and/or the Solution nor attempt to do any such thing except to the extent that (by virtue of sections 50B and 296A of the Copyright, Designs and Patents Act 1988) such actions cannot be prohibited because they are necessary to decompile the Software and/or the Solution to obtain the information necessary to create an independent program that can be operated with the Software, the Solution or with another program ("Permitted Objective"), and provided that the information obtained by you during such activities:

1.3.5.1. is not disclosed or communicated without our prior written consent to any third party to whom it is not necessary to disclose or communicate it in order to achieve the Permitted Objective;

1.3.5.2. is not used to create any software that is substantially similar in its expression to the Software;

1.3.5.3. is kept secure; and

1.3.5.4. is used only for the Permitted Objective

1.3.6. Publish, sell, distribute, broadcast, transmit, communicate, transfer, rent, lease, assign, display, disclose, pledge, share, licence or otherwise commercially exploit the Solution;

1.3.7. Grant any third party access to or use of the Solution or use the Solution for the benefit of any third party;

1.3.8. Access or use the Solution other than in accordance with this Appendix 2, the other terms of your Agreement or any terms of use set out on the Website or otherwise made available to you;

1.3.9. Install any Software on any operating system not supported by us; and/or

1.3.10. Remove any copyright, trademark or other proprietary notices from the Software.

1.4. By using the Solution you:

1.4.1. Agree and acknowledge that it is your responsibility at all times to back-up any data, software, information or other files stored on any Device;

1.4.2. Confirm that the Solution may include recommendations in relation to: software installation, configuration or updates; operating system updates or configuration; amendments to Device, router, firewall or security settings or configuration; password reset or amendment; or removal, amendment or alteration of data stored on your Devices;

1.4.3. Confirm that we may remove and install software, change Device settings and otherwise configure your Devices;

1.4.4. Acknowledge and agree that we may run security scans against your Devices;

1.4.5. Acknowledge and agree that we may from time to time provide Updates without requesting or obtaining your separate consent;

1.4.6. Acknowledge and agree that you may not be able to use the Solution or part of the Solution unless you use the latest Updates we have provided;

1.4.7. Authorise us to download and install on your Devices software programs that enable us to access and control your Devices remotely; and

1.4.8. Acknowledge and agree that we shall not be liable (whether such liability arises in contract, tort (including negligence), breach of statutory duty or otherwise howsoever arising) under any circumstances for any damage, loss, alteration or corruption of any data, information, software, files or any Device resulting from your use of the Solution.

1.5. For the avoidance of doubt, the Solution does not affect your responsibility to comply with PCI DSS.

2. Licence Terms for Secured Encrypt

2.1. Subject to the terms of this Appendix 2, we, grant you a non-assignable, non-exclusive, revocable, limited and non-transferable licence to use the Solution on your Device(s) during the Subscription Period.

2.2. You will not, and will not permit any third party to:

2.2.1. Disclose any licence or authorisation number for Solution to any party other than to us or our authorised representatives;

2.2.2. Circumvent or attempt to circumvent controls on the installation or use of the Solution;

2.2.3. Copy, modify, change, alter, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Solution in any form or media or by any means nor attempt to do any such thing;

2.2.4. Reverse compile, disassemble, translate, reconstruct, transform, extract, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Software and/or Solution nor attempt to do any such thing except to the extent that (by virtue of sections 50B and 296A of the Copyright, Designs and Patents Act 1988) such actions cannot be prohibited because they are necessary to decompile the Software and/or Solution to obtain the information necessary to create an independent program that can be operated with the Software and/or Solution or with another program ("Permitted Objective"), and provided that the information obtained by you during such activities:

2.2.4.1. is not disclosed or communicated without our prior written consent to any third party to whom it is not necessary to disclose or communicate it in order to achieve the Permitted Objective;

2.2.4.2. is not used to create any software that is substantially similar in its expression to the Solution;

2.2.4.3. is kept secure; and

2.2.4.4. is used only for the Permitted Objective;

2.2.5. Publish, sell, distribute, broadcast, transmit, communicate, transfer, rent, lease, assign, display, disclose, pledge, share, licence or otherwise commercially exploit the Solution;

2.2.6. Grant any third party access to or use of the Solution or use the Solution for the benefit of any third party; and/or

2.2.7. Access or use Secured Encrypt other than in accordance with this Appendix 2, the other terms of your Agreement or any terms of use set out on the Website or otherwise made available to you.

2.3. By using the Solution you:

2.3.1. Confirm that the Solution may include recommendations in relation to: software installation, configuration or updates; operating system updates or configuration; amendments to Device, router, firewall or security settings or configuration; password reset or amendment; or removal, amendment or alteration of data stored on your Devices;

2.3.2. Confirm that we may remove and install software, change Device settings and otherwise configure your Devices;

2.3.3. Acknowledge and agree that we may run security scans against your Devices;

2.3.4. Acknowledge and agree that we may from time to time provide Updates without requesting or obtaining your separate consent;

2.3.5. Acknowledge and agree that you may not be able to use Secured Encrypt or part of this Solution unless you use the latest Updates we have provided;

2.3.6. Authorise us to download and install on your Devices software programs that enable us to access and control your Devices remotely; and

2.3.7. Acknowledge and agree that we shall not be liable (whether such liability arises in contract, tort (including negligence), breach of statutory duty or otherwise howsoever arising) under any circumstances for any damage, loss, alteration or corruption of any data, information, software, files or any Device resulting from your use of the Solution.

2.4. For the avoidance of doubt, the Solution does not affect your responsibility to comply with PCI DSS.

Annex B To Appendix 2. – Set Up, Description And Technical Details

Elavon Secured Pro	Set Up	Description	Technical Details
PCI DSS External Vulnerability Scan	Outbound call* made by Elavon to configure the scan with customer and walk through SAQ	The purpose of this scan is to identify if there are vulnerable entry points to your business network by scanning all possible points of entry.	• Scans against two (2) IP addresses per MID only • Unlimited scanning on those two IPs • Required on a quarterly basis for PCI • DSS compliance • Scan report compliance remediation recommendations
Network Perimeter Scan	Outbound call* made by Elavon to configure the scan with the customer	The Network Perimeter Scan checks for possible entry points in your business network that could allow hackers to gain access to your businesses, potentially stealing your Purchasers' payment card information and other sensitive data.	• No software install is required • An Assurance badge will be available to display on your website • Scans against two (2) IP addresses per MID only
POS Application Discovery	Outbound call*made by Elavon to configure with the customer	When run on a regular reoccurrence, this scan cross checks and verifies your POS Application against the PCI Security Council list of approved POS Applications to ensure your compliance for requirements 6.1 and 11.2.1.	• Delivered via Sysnet Protect App – this needs to be downloaded to the device • Runs on Windows • Scans against two (2) Devices per MID only
Device Security Scan	Outbound call*made by Elavon to configure with the customer	The Device Security Scan can be used across PCs and laptops running Windows or OS/X operating systems and mobile devices running iOS or Android operating systems. The scan detects any stored purchaser card information and it also analyses the system for any current cyber-threats, viruses and malware. The scan will also check the overall computer security patch levels within the operating system and major software applications.	• Device Security Scan is delivered via the Sysnet Protect App the desktop version will be emailed to you and the mobile version can be downloaded from iTunes or Google Play Store • Scans your devices for vulnerabilities • Assess threats and vulnerabilities for operating system (OS) versions as well as other applications on your Device • Scans the following for unencrypted cardholder data to greatly reduce the risk of a data breach: Device and local memory, file contents • Scans many file types, including .xls(x), .doc(x), .ppt(x), .pst, .pdf, .zip, .txt, .csv, .html, .xml, .rtf, .odt, .sxw, .sql. and .pdf Windows, Mac OS X and Linux Mobile Device Security Scan is iOS and Android compatible Scans against two (2) Devices per MID only

*Outbound calls will be made approximately 15 days from Elavon's acceptance of your Application.

Annex B To Appendix 2. (continued)

Elavon Secured Pro	Set Up	Description	Technical Details
Cardholder Data Scan	Outbound call* from Elavon to configure with customer	The Cardholder Data Scan, will help you find unencrypted credit card numbers (also known as Primary Account Numbers 'PAN') on computers, laptops and tablets and other connected devices. This dramatically reduces the scope of your PCI DSS assessment by identifying where you store payment card data so that you can securely remove it.	• Delivered via Sysnet Protect App – needs to be downloaded to device • Low system impact • Displays files and folders containing suspected PAN data • Scans a wide variety of file types, including .xls(x), .doc(x), .ppt(x), .pst, .pdf, .zip, .txt, .csv, .html, .xml, .rtf, .odt, .sxw, .sql. and .pdf • Windows, Mac OS X and Linux • Scans against two (2) Devices per MID only
Antivirus Protection	Outbound call*made by Elavon to configure with the customer	Ensure your devices are not infected with viruses and other malware which can disrupt and potentially damage your business. Protect against a range of problems from inconvenient malware which can slow systems to preventing against hackers and phishing of your devices.	• Installed from a link that will be emailed to you • Support for one Device per MID only • Windows (all versions, Mac OS (all versions), Linux or Android operating systems

*Outbound calls will be made approximately 15 days from Elavon's acceptance of your Application.

Appendix 3. Unregulated Hire Terms

1. General

1.1. The following terms and conditions in this schedule apply whenever you hire Terminals from Elavon, except where you qualify for the Regulated Hire Terminal Terms and are in addition to the terms set out in the Agreement.

1.2. The agreement relating to your hire of the Terminals from Elavon consists of:

1.2.1. the provisions relating to the Terminals as set out in the Application Form (including without limitation the minimum hire period) accepted by us or as otherwise agreed in writing from time to time; and

1.2.2. the provisions relating to the Terminals as set out in the Schedule of Fees (including without limitation the pricing) accepted by us or as otherwise agreed in writing from time to time; and

1.2.3. the following hire terms and conditions set out in this schedule (together the "Unregulated Terminal Hire Terms").

1.3. Elavon will install or cause to be installed, and you will accept on hire for a rental period of, unless stated otherwise in your Application Form, a period of thirty-six (36) months commencing on the date of delivery (the "Minimum Hire Period") and continuing thereafter until and unless terminated earlier in accordance with paragraphs 1.10 or 1.11 below or terminated in accordance with section 25 of the Agreement.

1.4. You agree to accept delivery of the Hired Terminals within 28 days of us notifying you (which may be by email) that these are ready for delivery. If for any reason you fail to accept delivery within this timeframe then an administration fee of £100 plus VAT will be charged and be payable by you in accordance with the Agreement.

1.5. In return for Elavon providing the services set out under this schedule, the rental fees and any repair or replacement charges payable by you for Terminals supplied by Elavon will be debited to the Merchant Bank Account on a monthly basis by direct debit.

1.6. The placement of a Terminal on your locations shall be agreed between the parties. Elavon reserves the right to withhold or withdraw its agreement or consent to the placement of the Terminals, in the event of the locations being, or becoming, unsatisfactory for that purpose. For the avoidance of doubt, any Terminal provided to you by Elavon pursuant to a separate hire agreement (either Regulated Hire Terminal Terms or Unregulated Terminal Hire Terms) must be attended by the Merchant at all times during its operation.

1.7. You shall provide, maintain and pay for all power and telecommunications connections necessary to operate the Terminals including, payment for all related charges incurred by you in gaining access to and using the Merchant Services. You shall not use, or permit to be used, the SIM card from any GPRS Terminal for any purpose other than the transmission and receipt of data in connection with the Merchant Services. If you do so in breach of this paragraph 1.5, then you shall be liable for all additional voice call and/or data transmission charges incurred plus an administrative charge to cover all costs incurred by us in recovering those additional charges from you.

1.8. You will operate the Terminals in accordance with the Operating Guide and keep the Terminals clean, free from damage and misuse, safe, secure and not left unattended (unless authorised in writing by Elavon), and you shall notify Elavon promptly if any repair to any Terminal or a replacement Terminal is required. You shall not repair or attempt to repair or disassemble any Terminal. Any damage to, or malfunction of, the Terminals resulting through the use of non-approved equipment and materials, or from your attempt to repair or disassemble, will be your responsibility. You agree that Elavon shall not be held liable for any Claims or Loss suffered by you as a result of your failure to comply with Paragraph 1.8.

1.9. You shall replace or upgrade the Terminals as Elavon or the Card Schemes may require from time to time. If any repair or replacement of a Terminal is required due to damage or misuse of the Terminal or the Terminal is lost or stolen, then Elavon shall have the right to recover from you the cost of such repair or replacement. Elavon's decision as to whether the repair or replacement is due to damage or misuse, or the Terminal has been lost or stolen shall be final and binding.

1.10. You acknowledge and agree that due to the nature of wireless technology, certain limitations exist that may affect the performance, Coverage Area and reliability of wireless technology and wireless processing in relation to a Card Reader or other Wireless Terminal. In the event that your ability to process wireless Transactions is limited or prevented for any reason, you agree not to use the Wireless Terminal and instead, to process the Transaction using alternative means as set out in the Operating Guide.

1.11. If you fail to pay any amount under or in connection with this Unregulated Terminal Hire Terms when due then in addition to any other rights herein (including our right to terminate) we may:

1.11.1. switch off the Hired Terminals until payment is made;

1.11.2. re-possess the Hired Terminals;

1.11.3. exercise our rights of withholding, deduction or set-off as described in clauses 14 and 15 of the Agreement above;

1.11.4. charge you interest on a daily basis on the overdue amount in accordance with clause 26.5 of the Agreement;

1.11.5. charge you any reasonable costs and expenses incurred by Elavon in endeavouring to collect any unpaid and overdue instalments, including any debt collection agency charges and reasonable legal costs which are incurred by us in exercising our rights under this Agreement, including enforcement of it; and

1.11.6. register the default with a credit reference agency, which may impact your ability to obtain credit in the future.

1.12. The Hired Terminals remain the property of Elavon. You shall not sell, charge, encumber, part with possession or otherwise dispose of the Hired Terminals. You will insure against loss or damage to the Hired Terminals including without limitation for the full replacement value in the sum of £500 for each of the Hired Terminals supplied to you. If you receive any insurance monies you must hold these on trust for Elavon.

1.13. You must return each Terminal to Elavon within ten (10) Business Days following termination of the Agreement or Unregulated Terminal Hire Term.

1.14. Where these Unregulated Terminal Hire Terms have terminated (for whatever reason) prior to the expiry of the Minimum Hire Period or any subsequent renewal (as the case may be), then in addition to the provisions of paragraphs 1.6 above, you will immediately pay Elavon

1.14.1. all arrears of rental payments outstanding at the date of termination;

1.14.2. a sum equal to the aggregate of all rental payments which would, but for the termination of the Agreement or Unregulated Terminal Hire Term, have become due and payable under the Unregulated Terminal Hire Terms from the date of termination to the expiry of the Minimum Hire Period.

1.14.3. a Terminal Recovery Fee, which is an administrative charge only, payment and acceptance of which shall not amount to a waiver of damages, compensation or other fees due to Elavon; and

1.14.4. in the event that any such Terminal is not returned, Elavon will charge you the cost of replacing that Terminal in addition to the Terminal Recovery Fee.

1.15. Where Elavon has charged for the replacement cost of the Terminal in accordance with paragraph 1.13.3, Elavon may shall refund the amount to you upon receipt by Elavon of the Terminal in satisfactory condition and good working order, free from damage.

1.16. You carry the risk of Terminals in transit so that if any Terminal is lost or returned to Elavon in a damaged condition, Elavon may charge you an appropriate amount to cover any repairs or replacement of that Terminal.

1.17. You agree that we may assign, novate, transfer or subcontract any or all of our rights and obligations under this schedule and/or ownership of the Hired Terminals to a third party at any time without your consent. You shall execute any document reasonably required by us to give effect to any such assignment, novation or subcontracting.

1.18. Paragraphs 1.4, 1.5, 1.11, 1.12, 1.14, 1.15, 1.16, 1.19 and 1.20 and such other clauses as by their nature are intended to survive termination, will continue to apply in respect of the Hired Terminals following termination of these Unregulated Terminal Hire Terms for whatever reason.

1.19 If you are a partnership, each partner will be jointly and severally liable under the Unregulated Terminal Hire Terms.

1.20. We shall not be liable for any delay or failure to carry out any of our obligations under the Unregulated Terminal Hire Terms if such failure is due to circumstances beyond our direct control.

1.21. These Unregulated Terminal Hire Terms are personal to you and you may not assign or transfer them. If you are an individual, the Unregulated Terminal Hire Terms will be binding upon your personal representatives.

Appendix 4. Goods

Part A: Terms Applicable to Goods (Including Card Readers)

1. Delivery and/or Installation Of Goods

1.1. Where Goods are to be installed (as indicated in the Application), we shall agree a timetable for the installation of the Goods with you. Elavon shall use reasonable endeavours to install the Goods in accordance with the timetable however, you agree that time of installation is not of the essence and may not be made so by the service of any notice.

1.2. Save for where installation is selected in the Application, we shall deliver the Goods to you at the address you specified as your Trading (DBA) Address in the Application. Any dates suggested for delivery of the Goods(s) are estimates only and time of delivery is not of the essence and may not be made so by the service of any notice.

1.3. Subject to paragraph 1.4 below, Elavon shall not be liable for any loss incurred by you if the delivery or installation of the Goods is delayed for any reason from the anticipated delivery or installation date.

1.4. If Elavon fails to deliver or install the Goods within 30 days of us notifying you in writing that your Application has been accepted and (i) you notify Elavon as soon as possible after the anticipated delivery or installation date that delivery has not occurred; and (ii) we have had the opportunity to make another delivery or installation; and (iii) delivery or installation has not failed due to any action or omission by you, including your failure to sign for the Goods (if applicable) or your refusal to accept delivery or installation; then Elavon's obligation shall be limited to the value of a refund of the purchase price of the Goods.

1.5. If you fail to accept installation of, or take delivery of the Goods, then except where such failure or delay is caused by Force Majeure or by Elavon's failure to comply with our obligations under the Agreement in respect of the Goods:

1.5.1 installation or delivery of the Goods (s) shall be deemed to have been completed at 9:00 am GMT on the third Business Day following the day on which Elavon attempted to make the first installation or delivery of the Goods (notwithstanding any further attempts Elavon makes to install/deliver the Goods after the first attempt); and

1.5.2. Elavon shall store the Goods until installation or delivery takes place and charge you for all related costs and expenses (including insurance).

1.6. If ten (10) Business Days after Elavon attempted to make the first delivery or installation of the Goods you have not accepted installation or taken delivery of the Goods or notified us that delivery/ installation has not taken place (notwithstanding any further attempts Elavon makes to deliver, or install, the Goods at our discretion), Elavon may resell or otherwise dispose of the Goods. Elavon shall be entitled to treat the Agreement as having been terminated by you ten (10) Business Days after we attempted to make the first installation or delivery of the Goods and Elavon reserves the right to charge a reasonable administrative fee to you in respect of your termination.

1.7. Elavon shall not be liable for any delay or failure in delivery or installation in the event of Force Majeure or your failure to provide us with adequate delivery instructions for the Goods or any relevant instruction relating to the supply of the Goods.

1.8. The risk of loss, theft or damage to the Goods shall pass to you on completion of delivery or installation, as applicable.

1.9. Notwithstanding delivery or installation of the Goods, title to the Goods shall not pass to the Customer until payment in full of the Fees due in respect of the Goods, in accordance with this Agreement.

2. Disposal Of Goods

2.1. We are committed to meeting the requirements of the European Union (Waste Electrical and Electronic Equipment) Regulations 2014. These Regulations require producers of electrical and electronic equipment to finance the takeback of WEEE resulting from products that we place on the market. This helps us to ensure that WEEE is reused or recycled safely. In line with that commitment Elavon Merchant Services will take back WEEE from you. Please contact us for details.

You also have a role to play in ensuring that WEEE is reused and recycled safely. So, if you choose not to return WEEE to us then you should not dispose of it in your bin. The crossed out wheeled-bin symbol on the product reminds users not to dispose WEEE in the bin. You should ensure that the WEEE is collected separately and sent for proper treatment. WEEE contains hazardous substances and if not managed and treated safely it can cause pollution and damage human health.

Part B: Terms Applicable to Card Readers

1. Quality of Card Readers

1.1. Elavon warrants that on delivery, and for a period of twelve (12) months from the date of delivery (the "Warranty Period") the Card Readers shall:

1.1.1. conform in all material respects with its description;

1.1.2. be free from material defects in design, material and workmanship;

1.1.3. be of satisfactory quality (within the meaning of the Sale of Goods Act 1979, as amended); and

1.1.4. be fit for any purpose held out by Elavon.

1.2. Except as explicitly provided in this paragraph 1, in relation to the supply of Card Readers, all warranties, conditions and other terms implied by statute or common law are, to the fullest extent permitted by law, excluded from the Agreement. For the avoidance of doubt, the warranty set out in paragraph 1.1 above excludes, in particular, costs arising from not being able to use the Card Reader or from damage or loss caused when the Card Reader breaks down; and the cost of replacing any items or accessories that are intended to be replaceable, such as batteries, cables, power suppliers and plugs.

1.3. Subject to this section 1, if during the Warranty Period the Card Reader does not comply with the warranty set out in paragraph 1.1 above and you notify Elavon and (if asked to do so) return such Card Reader (within a reasonable time of discovery of the defect) to the address notified to you by Elavon at your cost, then Elavon shall, at its option, having examined the Card Reader, repair or replace the defective Card Reader, or refund the purchase price of the defective Card Reader in full.

1.4. Elavon shall not be liable for the Card Reader's failure to comply with the warranty in paragraph 1.1 above if:

1.4.1. the defect arises because you have failed to follow any instructions, including those set out in the TOS, Operating Guide, any Card Reader manual or good trade practice) as to the storage, installation, commissioning, use or maintenance of the Card Reader;

1.4.2. you are not using the Card Reader with a Compatible Device;

1.4.3. you alter or repair such Card Reader without Elavon's prior written consent;

1.4.4. you fail to return the Card Reader to Elavon for maintenance or, upon reasonable written notice from Elavon, fail to apply software downloads, updates and/or upgrades to the Card Reader at Elavon's direction;

1.4.5. the defect arises as a result of fair wear and tear, including cosmetic damage, or your wilful damage, negligence or abnormal working conditions or use in conjunction with items not approved by Elavon.

1.5. Elavon shall have no liability to you in the event that the Card Reader is required to be replaced or modified in any way as a direct result of any change in the Card Scheme Rules, including PCI DSS, and you agree to return the Card Reader to Elavon at our written request. You acknowledge and accept that Elavon will be required to discontinue use of any Card Reader which is no longer compliant with Card Scheme Rules, including PCI DSS, and that you are responsible for purchasing any replacement Card Reader(s) to ensure continued compliance with these requirements.

1.6. The TOS shall apply to any repaired or replacement Card Reader supplied by Elavon under subsection 1.1 although any warranty in respect of a repaired or replacement Card Reader will apply only for the remainder of the Warranty Period which is unexpired in respect of the first Card Reader.

2. Security

2.1. You are responsible for taking all reasonable security measures to keep the Card Reader safe, including measures to prevent unauthorised use of it. If you know or suspect that the Card Reader has been lost, stolen or misused, you must notify Elavon immediately

2.2. You are responsible for ensuring that the Card Reader is not accessed or used to commit any fraud or theft by you, the Cardholder or any third party while the Card Reader is in your possession. You will be liable for any losses that result from such criminal acts, if they occur as a result of either:

2.2.1. Your or your employees' negligence; or

2.2.2. Your non-compliance with the TOS, Operating Guide, any Card Reader manual or good commercial practice to prevent fraud and/or theft.

2.3. Elavon may block use of the Card Reader if:

2.3.1. Elavon has reasonable grounds for concern about the security of the Card Reader;

2.3.2. Elavon has reasonable grounds to suspect that it has or may be used for a fraudulent or criminal purpose or in an unauthorised manner;

2.3.3. Elavon suspects or has reasonable grounds to believe that the Card Reader is being used outside the United Kingdom; or

2.3.4. Elavon is obliged to do so to comply with legal or regulatory obligations howsoever arising. Elavon shall notify you of any such action, and the reasons and the procedures for rectifying any factual errors that have led to the action unless Elavon is prohibited from doing so under the Laws. Elavon may charge you the reasonable costs of any such notification.

ELAVON TOS – UK Operating Guide 05/2025

Table of Contents