CASTLES TECHNOLOGY

Castles Technology V3C and V3M2

User Manual

Introduction
Vega 3000 terminal family

Thank you for choosing your new Castles Technology terminal.
The terminal range offers simple operation combined with the ability to perform fast and secure payment transactions. Please read through this User Manual which contains important information to help you install, use and maintain your payment terminal. Content includes step-by-step guides for all the transaction types, running reports and end-of-day procedures.

Introduction
Countertop Vega 3000 (V3C)

Castles Technology manufacture a wide range of terminals to meet all retail environments:

Countertop terminal Vega 3000 (V3C)

The V3C terminal is designed to operate on a countertop. The terminal is powered by a mains power supply.

Countertop terminal
V3C Countertop

Power supply
Mains power supply

Communication method
Via the Internet and/or analogue phone line

Vega 3000 Portable

Portable terminals Vega 3000 GPRS (V3M2 GPRS) and Vega 3000 Wi-Fi (V3M2 Wi-Fi)

The Vega 3000 GPRS (V3M2 GPRS) and Vega 3000 Wi-Fi (V3M2 Wi-Fi) terminals have been designed to meet the needs of those merchants requiring portable payment. In the case of the V3M2 Wi-Fi , this is designed to be used in a shop or restaurant. The V3M2 GPRS is completely mobile and utilises the 3G technology. Both the V3M2 Wi-Fi and V3M2 GPRS are powered by an internal lithium battery.

The V3M2 Wi-Fi and V3M2 GPRS have the option of being supplied with a charging stand, but an alternative charging solution is to plug a USB Type B cable into the terminal. The option provided with your V3M2 Wi-Fi and V3M2 GPRS will depend on the agreement with your terminal leasing company.

Portable Terminal
V3M2 GPRS

Power supply
Battery module with mains powered charging stand or via USB cable.

Communication method
Wi-Fi

Portable Terminal
V3M2 GPRS and WIFI

Power supply
Battery module with optional mains-powered charging stand or via USB cable

Communication method
GPRS / 3G

Safety information and battery guarantee

General safety information

- Do not use if visibly damaged.
- Do not apply power/operate below 0 °C and above 50 °C.
- Do not store in an unpowered state below –20 °C and above 70 °C.
- Do not expose to moisture and do not store or operate in high-humidity environments.
- Do not disassemble.
- Do not incinerate or crush.
- This product is not suitable for use in hazardous environments such as petrol stations, chemical depots, etc.
- Keep out of reach of children and pets.
- Recharge the battery module only with the supplied power supply or charging stand.
- Do not short-circuit battery module contacts by placing metal objects across the connections.
- Use only batteries supplied by Castles Technology as a replacement

Battery module safety for the V3M2 portable terminals

- Do not drop or impact
- Do not disassemble, puncture or breach.
- Do not leave in direct sunlight.
- Do not moisten or throw into water.
- Keep any spare batteries in a cool, dark, dry place out of direct sunlight
- Do not expose to fire or incinerate.
- Never expose to temperatures less than –20 °C or greater than 70 °C. You must dispose of used or faulty batteries using either your local battery disposal facility in accordance with local laws, or by return to Castles Technology. Do not discard with general waste and do not incinerate. Insulate the battery module contacts with electrical tape prior to disposal. This battery module is a lithium-ion battery.

Safety information and battery guarantee (cont.)

General caution and safety instructions

- Do not attempt to disassemble, service or repair any part.
- Do not use if damaged or with signs of tampering.
- Only use the supplied power adapter provided by Castles Technology or from the official supplier, ensuring correct rating.
- To avoid the potential hazard of electrical shock do not use in wet environments or during an electrical storm.
- Do not use in the proximity of potentially flammable gases or substances.
- Ensure cables used do not cause a trip hazard or risk the device being dropped on to a hard surface.
- Do not expose to excessive heat or cold. Only operate between 0 °C and 50 °C.
- Before cleaning disconnect from electrical outlet. Use only a dry or dampened soft cloth.
- Do not immerse, use liquids, sprays or aerosol cleaners. Clean all spillages quickly.
- This device is intended for handheld use only (V3M Wi-Fi and V3M GPRS terminals).
- Dispose any part in an environmentally sound manner and in accordance with local laws. Castles Technology will not be held liable for any damage resulting from user operation that does not comply with the guidance stated.

Castles Technology will not be held liable for any damage resulting from user operation that does not comply with the guidance stated.

How to Clean Your Terminal

WARNING: DO NOT USE UNDILUTED AMMONIA OR ABRASIVE CLEANERS

Switch off and unplug the mains power supply units from the terminal, PIN Pad, charging stand and Wi-Fi access point where applicable. Carefully note how all the cables are connected and disconnect all cables before cleaning.
Apply denatured alcohol (methylated spirits) to a clean, soft, non-abrasive, low-lint cloth. Wipe carefully.
Use an air duster (compressed air) to clean in and around the printer mechanism.

Safety information and battery guarantee (cont.)

Battery module guarantee

- Unless the terms & conditions of your terminal supply differ, the battery module is excluded from the Castles Technology terminal warranty and is guaranteed for one year. If your battery module fails after this period you must purchase a replacement battery module from Castles Technology.
- Battery module performance does degrade over time and you will need to purchase a replacement when the battery module performance becomes unacceptable.

PCI-PTS

PCI SSC's approval only applies to PEDs that are identical to the PED tested by a PCI Security Standards Council recognized laboratory. If any aspect of the PED is different from that which was tested by the laboratory – even if the PED conforms to the basic product description contained in the letter — the PED model should not be considered approved, nor promoted as approved. For example, if a PED contains firmware, software, or physical construction that has the same name or model number as those tested by the laboratory, but in fact are not identical to those PED samples tested by the laboratory, then the PED should not be considered or promoted as approved.
No vendor or other third party may refer to a PED as "PCI Approved," nor otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a vendor or its PEDs, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in an approval letter. All other references to PCI SSC's approval are strictly and actively prohibited by PCI SSC. When granted, an approval is provided by PCI SSC to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but the approval does not under any circumstances include any endorsement or warranty regarding the functionality, quality, or performance of any particular product or service. PCI SSC does not warrant any products or services provided by third parties. Approval does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services, which have received an approval, shall be provided by the party providing such products or services, and not by PCI SSC or the payment brand participants.
EU Compliance Statement: Castles Technology hereby declares that this device is in compliance with the essential requirements and other relevant provisions of the R&TTE Directive.
A copy of the EU Declaration of Conformity is available online.

Additional services available for your terminal

Card types accepted
The terminal is configured as standard to support Visa and Mastercard scheme credit and debit cards. For some merchant categories, credit card support may not be allowable. The terminal can support American Express, Diners Club, UPI and JCB scheme cards depending upon your bank agreements with these schemes.

Sale (Purchase) with cashback
The terminal can be configured to offer Sale with Cashback.

Tipping
The terminal can be configured for a tipping service.

Pre-authorisations (hotel and rental)
The terminal can be configured for Pre-Authorisations and Completion transaction types that are widely used in the hotel and rental business sectors.

Purchase/Sale with Reference number
This feature allows entry of a reference number such as invoice, table or room number to your receipts.

Customer Not Present
The terminal can be configured for taking transactions when the cardholder is not next to the terminal - a mail order or telephone order (MOTO), for example.

Please contact your terminal leasing company if you require any of the above additional services. The above configuration options are only available if permitted by your bank.

Table of contents
Page directory

Table of contents
Page directory

Important information

Terminal Identification (TID)
Each terminal contains an electronically programmed eight digit number known as a Terminal Identifi-cation (TID. This is printed in full on the merchant's copy of all transaction receipts.

Merchant Identification (MID)
Your bank will have issued you with a MID, supplied in a separate documentation pack directly from them. If you do not have this number, please contact your bank.

Before taking transactions you should confirm the MID printed on your Terminal Report matches the MID issued by your bank. If not, please contact your helpdesk. You may have separate MIDs for Amer-ican Express, Diners Club, JCB, and Duet cards, and the mobile Top Up service, if you have requested these.

Merchant (Local) Password
Your terminal contains a merchant password that you are encouraged to change from the default setting. Please refer to the password section for a full explanation.

Voice Referral Password
Your terminal may require a voice referral password that you are encouraged to change from the de-fault setting. If applicable, please refer to the separate password documentation for a full explanation.

RECEIPT: The inclusion of a * symbol printed on the Merchant Copy of the transaction receipt indicates that the transaction was authorised using the Voice Referral process.

Operator ID
Your terminal may require you to input an Operator ID during a Voice Referral transaction. The Operator ID will be provided by the Authorisation centre.

RECEIPT: The inclusion of a * symbol printed on the Merchant Copy of the transaction receipt indicates that the transaction was authorised using the Voice Referral process.

'Batch' end-of-day banking (settlement)
At the end of each business day, the Settlement procedure **must** be performed on the terminal. If you do not complete this procedure you may experience delays in funds being transferred to your bank account.

Cash Register Interface
If you have an SP terminal or PIN Pad integrated with your cash register/till system, many of the func-tions of the terminal will be carried out by cash register functions.

Certain functions described in this user manual may not be available via the cash register interface.

If your terminal operates in conjunction with a cash register, your head office or the product manufac-turer will have provided additional instructions.

Data Security Standard (PCI DSS) advice

Monthly Updates
Once a month your terminal will connect to the Castles Technology Terminal Management System to download any new software and any important configuration changes. This update will typically occur during the night. For this reason, Castles Technology recommends you leave your terminal powered on at all times. If you have a portable device, we recommend it is left on the charging stand or connected to the power supply when not in use. In the event of a terminal being switched off when the update tried to take place (or having a flat battery in the case of portable models), it will notify you that it has failed. Please leave your terminal on the following night to ensure the upgrade is completed, or call your helpdesk for assistance. These calls will be charged should your terminal use a dial-up connection method. Charges may vary depending on your phone provider.

The Castles Technology Vega 3000 terminal family contains a payment application that stores, processes and transmits cardholder data. It therefore falls within the scope of the Payment Card Industry Data Security Standards (PCI DSS).

This section contains advice to assist you with PCI DSS compliance.

Please note it is the responsibility of the merchant to ensure the merchant copies of receipts and reports showing cardholder details are stored securely for the period of time specified by your bank. Please also ensure they are disposed of in a secure manner at the end of that period. Failure to do so may result in charge-backs or fraudulent activity.

1. Retention of full magnetic stripe, card validation code or PIN block data
The payment application within the Castles Technology Vega 3000 family of terminals does not retain such data. You need take no further action to ensure your PCI DSS compliant environment meets this specific requirement.

2. Protection of stored cardholder data
The payment application within the Castles Technology Vega 3000 family of terminals protects stored cardholder data in a secure manner.

You must ensure you give the correct copy of the receipt to the cardholder (clearly marked CARDHOLDER COPY) and retain the merchant receipts in a secure area with limited access to authorised staff. The merchant receipts must be destroyed by incineration or by cross-shredding when they become obsolete. Your bank will advise on the period necessary for retention of receipts.
You should perform an End of Day Banking/Settlement every day. Your terminal may be configured to perform this process automatically every day; if you are unsure how your terminal is configured, please contact your helpdesk.

3. Provision of secure authentication features
The payment application operates in the Castles Technology Vega 3000 hardware environment and does not require username or password access. You need take no further action to ensure your PCI DSS compliant environment meets this specific requirement.

Data Security Standard (PCI DSS) advice

4. Secure payment applications
The Castles Technology Vega 3000 terminal and its software applications have been designed in line with PCI DSS and industry best practices. You need take no further action to ensure your PCI DSS compliant environment meets this specific requirement.

5. Protection of wireless transmissions
The Castles Technology V3M2 Wi-Fi utilises Wi-Fi wireless transmissions in accordance with PCI DSS and industry best practices.

6. Testing payment applications to address vulnerabilities
Castles Technology have a process to identify newly discovered security vulnerabilities and have timely development and deployment of security patches and upgrades. You need take no further action to ensure your PCI DSS compliant environment meets this specific requirement.

7. Secure network implementation
The payment application operates in the Castles Technology Vega 3000 family hardware environment and does not need to log application activity.

8. Ensuring cardholder data must never be stored on a server connected to the Internet
If you are using the Castles Technology Vega 3000 family device on a Local Area Network for the payment transaction interface and you are using a local server to store and forward the transaction data, you must take steps to protect the transaction data in accordance with DSS requirements.

9. Secure remote software updates
Software updates will be carried out automatically by the Castles Technology terminal management system. This system ensures only authenticated payment software is loaded onto your terminal.

10. Secure remote access to payment application
There is no remote access to the payment application.

11. Encryption of sensitive traffic over public networks
Transactions sent over network connections are always encrypted by the payment application using Secure Socket Layer (SSL) technology.

Transactions sent over network connections are always encrypted by the payment application using Secure Socket Layer (SSL) technology.
You must never communicate sensitive cardholder data by any means unless it is encrypted. Spire Payments will never request such data from you. Sensitive cardholder data means:

- the Card Number (often known as Primary Account Number orPAN),
- the Cardholder Name, the card Expiration Date,
- the card CV2 number (the last three digits printed on the card signature strip, or for American Ex-press, the four digit value printed on the front of the card).

Data Security Standard (PCI DSS) advice

Your helpdesk may request the first six digits of a card number from you to assist with troubleshooting a problem. This should be provided along with the name of the card issuer when requested, to enable your helpdesk to assist.
You will not be asked for a full card number by your helpdesk.

12. Encrypt all non-console administrative access
This is not applicable to the Castles Technology payment application.

13. Maintain instructional documentation/training programs for cardholders, resellers, & integrators
As well as the information in this user manual, Castles Technologys will make further information regarding PCI DSS compliance available to you via its website www.spirepayments.com.

Software license

Understanding your Vega 3000 Portable

Portable Terminals V3M2 GPRS and V3M2 Wi-Fi Overview

Four status LEDs
Refer to the contactless section on page 37 in this User Manual for details

Colour display
Displays merchant menu system and transaction progress

USB port
For charging the battery

Power button
Press button to turn the terminal on

Chip card reader
Use when the cardholder presents a chip card

Keypad
For merchant & cardholder data entry

Serrated paper cutter
Receipts will emerge from this slot and can be removed by pulling across the serrated cutter

Paper roll compartment
More information about your printer and how to load a paper roll can be found on page 17 in this User Manual and in the Quick Reference Guide

Swipe card reader
Use when the cardholder presents a debit or credit card without a Chip or when prompted by the terminal

Battery compartment
Battery replacement is detailed on page 16 in this User Manual and in the Quick Reference Guide

Understanding your Vega 3000 Countertop

Countertop Terminal V3C Overview

Four status LEDs
Refer to the contactless section on page 37 in this User Manual for details

Colour display
Displays merchant menu system and transaction progress

USB port
For connecting peripherals equipment

Power button
Press button to turn the terminal on

Chip card reader
Use when the cardholder presents a chip card

Keypad
For merchant & cardholder data entry

SIM/SAM compartment
Please do not open unless instructed

Serrated paper cutter
Receipts will emerge from this slot and can be removed by pulling across the serrated cutter

Paper roll compartment
More information about your printer and how to load a paper roll can be found on page 17 in this User Manual and in the Quick Reference Guide

Power supply socket
This is where the power supply plugs into the terminal

Terminal connections
This is where the telephone line, network and serial cables attach

Cable tidy
A removable clamp keeps cables in place & prevents disconnection

Swipe card reader
Use when the cardholder presents a debit or credit card without a Chip or when prompted by the terminal

Battery module portable terminals

If you have a portable terminal such as V3M2 Wi-Fi or GPRS it will use a removable, rechargeable lithium ion battery module. The battery module will need to be charged when you receive a new terminal, a replacement battery, and during day-to-day use. See appendix 'F' at the end of the document for further details.

Battery maintenance

It is recommended to always return the terminal to the charging base or connect to the power supply when not in use to maintain maximum charge. While handling the battery module ensure you do not short the connections with metallic objects.

Battery module installation and replacement

Step 1

Place the terminal face down on a flat surface and remove the battery cover by applying pressure on two tabs and pushing

Step 2

Remove any packaging and insert the battery into the terminal.

Step 3

Place battery compartment cover back into position.

Loading the paper roll

The Vega 3000 Mobile and Countertop terminals are all supplied with a paper roll. It may be loose in the box or can be found in the terminal's paper compartment. It is critical that only approved paper rolls are used and these can be obtained from authorised paper roll supplier.

Paper roll loading procedure

Step 1

With the terminal facing up, pull upwards on the lever located in the middle of the printer door.

Step 2

Discard any packing material from the paper roll. Place the roll in the compartment as shown in the diagram. The paper must feed from underneath the roll. The correct orientation of the paper is critical (if you experience blank receipts, the paper may be incorrectly inserted or of the wrong specification). Pull a length of paper until it protrudes from the top of the terminal.

Step 3

Close the printer door until an audible 'click' is heard.

Step 4

Remove the excess paper by pulling down and tearing along the serrated edge.

Cable connection V3C Countertop terminal

Step 1

Place the terminal face down on a flat surface

Step 2

Open the cable tidy bridge.

Step 3

Thread the black power supply cable to the right of the cable tidy recess and insert the plug into the rear of the terminal to 9V socket

Thread the network cable to the left of the cable tidy recess and insert the plug into the socket identified with LAN.
Alternatively, if you are connecting the terminal to a telephone connection point, thread the telephone cable through the cable tidy recess and insert the plug into the socket identified with the telephone symbol.

(IP with dial backup: Please note both a telephone and network cable can be connected simultaneously. Refer to page 75 of this user manual for more details).

Step 4

Refit the cable tidy until you hear a 'click'. Connect the network cable to your Internet connection point.
Connect telephone cable (if required)to the telephone socket.
Power: finally, connect the power supply to a live mains socket.

Communications information

Analogue phone line connections

The Vega 3000 Countertop (V3C) terminal utilises an analogue phone line (dial-up) and Internet connection to communicate with acquiring systems and the Castles Technology terminal management system. The choice of communication method will be dependent upon the configuration requested by the terminal leasing company. We recommend an Internet connection as the primary communication method, with an analogue phone line also connected as a back-up in the event of a network problem

The following points must be observed:

- Terminals using dial-up connections are designed for use on analogue telephone lines such as those provided by the Public Switched Telephone Network (PSTN) and some Private Branch Exchanges (PBX/PABX). These terminals will not operate on a proprietary digital telephone extension.
- The terminal will need to be configured (see Appendix E) if your line requires a prefix number to dial externally (a '9' is a typical example).
- Using double adaptors and/or extension cables may cause communication problems. Always use LAN and telephone cables supplied by Castles Technology
- Installing the terminal on a line using a third party call service may cause communication problems.

Broadband Internet access compatibility

If the telephone line you wish to use is also shared with other devices (including telephones), ensure all sockets are fitted with ADSL or DSL filters. This does not just apply to the socket your Internet access point is connected to.

Incorrect installation may cause communication problems.

Wired network (V3C terminal only)

The Vega 3000 Countertop (V3C) terminal can connect over a network connection via a local area network.

The Vega 3000 Countertop (V3C) terminal connection is on the back of the terminal LAN port).

This is connected to your Internet connection point (see previous section).

Communications information (cont.)

Vega 3000 GPRS (V3M2 GPRS) portable terminal only
The Vega 3000 M GPRS (V3M2 GPRS) communicates through the mobile telephone network using a 3G connection. A Subscriber Identity Module (SIM) is pre-installed into the terminal by Castles Technology to control this connection.

The following points should be noted:

- **Do not remove the SIM unless instructed by your helpdesk. Unauthorised removal of the SIM may render your terminal inoperable and/or may result in late/non-payment of funds into your account.**
- **Castles Technology reserves the right to charge for unauthorised use of your SIM. Castles Technology may charge an administration fee for misuse or replacement of a lost or locked SIM.**

Vega 3000Wi-Fi (V3M2 Wi-Fi) portable terminal only

Vega 3000 Wi-Fi (V3M2 Wi-Fi) is a portable device which utilises the wireless technology known as Wi-Fi. This is ideal for retail environments such as restaurants where waiters can take payment at the table.

To install the V3M2 Wi-Fi you must note the following:

- Your terminal will be pre-configured for use on standard networks featuring DHCP (automatic allocation of IP addresses). In the unlikely event that your network does not have this feature, you would need to contact your ISP or Interntet support team to obtain Static IP address, Subnet Mask, Gateway IP address and DNS IP address. Once all the details in hand please call your helpdesk for assistance with configuring this on your terminal.
- Please ensure the specific IP addresses and TCP ports provided by your terminal supplier are not blocked by a network firewall.

Wi-Fi access point

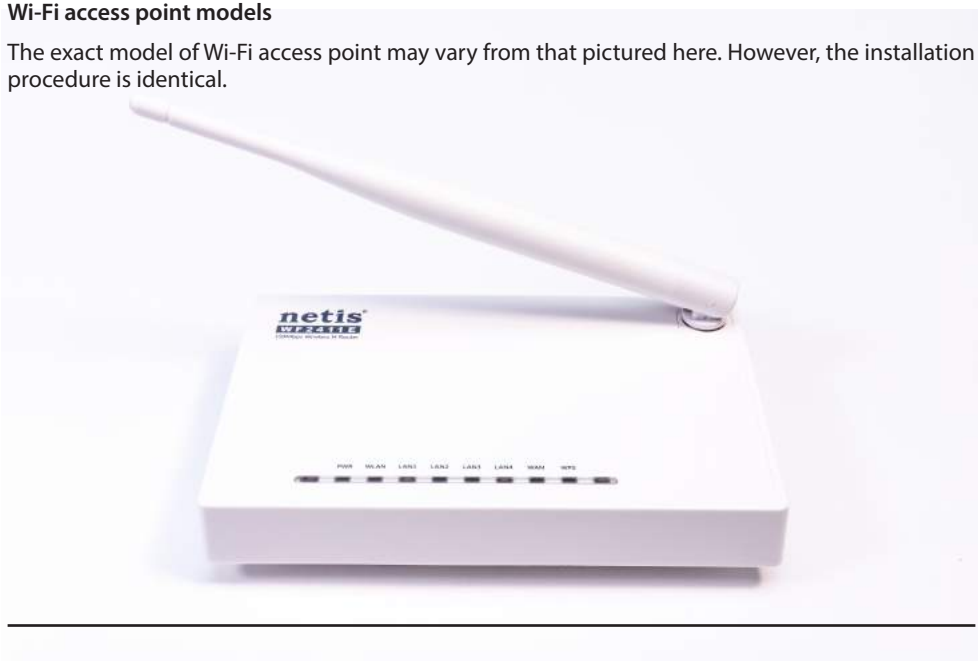
To operate the V3M2 Wi-Fi within your premises you may also be provided with a Wi-Fi access point. Both the Wi-Fi access point and terminal will be pre-configured with all the necessary information to allow the devices to communicate. Should the terminal or Wi-Fi access point be replaced or the link between the terminal and Wi-Fi access point fail, reconfiguration may be needed. See Appendix F for details of the Wi-Fi access point pairing procedure.

Please note: If you are not using the Castles Technology's provided Wi-Fi access point then you may have to configure your router to support the payment terminal, e.g. for MAC address filtering.

Wi-Fi (V3M2 Wi-Fi portable terminal only)

Wi-Fi access point models

The exact model of Wi-Fi access point may vary from that pictured here. However, the installation procedure is identical.



Wi-Fi access point siting recommendations

The design of the Wi-Fi access point allows it to be placed on a counter or shelf. It could be also installed on the wall.

Please bear the following in mind when choosing an installation location:

- Select a location close to an electrical power outlet.
- Select a location close to a network connection point.
- Select a location where there will be no physical obstructions between the Wi-Fi access point and the V3M2 Wi-Fi operating area. This includes brick and block walls.
- Do not install or place the Wi-Fi access point on a metal or metallised material surface.
- Avoid close proximity to cordless phones, Bluetooth devices, microwave ovens and other mobile devices.

Wi-Fi access point cable connection

Please follow this procedure carefully and only power on the terminal and Wi-Fi access point when instructed.

Step 1

Plug the supplied network cable into the WAN socket in the Wi-Fi access point. Connect the other end to the internet source.

Step 2

Plug the power supply into the Wi-Fi access point.

Step 3

Plug the Wi-Fi access point power supply into the mains power socket and switch on.

Note: Multiple V3M2 Wi-Fi terminals can communicate with a single Wi-Fi access point.

V3M2 Wi-Fi portable terminal's expected range

The range of a V3M2 Wi-Fi from the Wi-Fi access point should be in the region of 100 feet in all directions, but this can vary due to internal obstructions and potential interference from other equipment. (See page 21 for siting recommendations.)
Once the system is powered, it is best to carry the terminal to the extremes of your premises where you would expect to take payment and check operation. If necessary, relocate the Wi-Fi access point.
Alternatively, it is possible to boost the Wi-Fi signal strength by purchasing an aftermarket repeater.

Installation

Please read and follow the separate Quick Reference Guide and FAQ received with your terminal. This User Manual, F.A.Q. and the Quick Reference Guide contain instructions on how to:

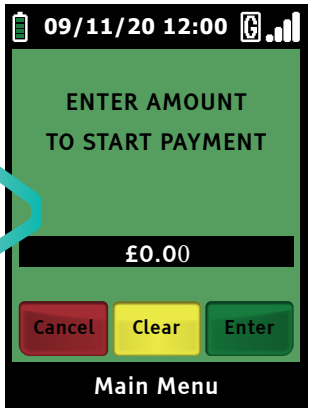
- Connect the cables and accessories, e.g. power supply, telecoms cable.
- Install the paper roll.
- Charge the battery module (V3M2 GPRS and V3M2 Wi-Fi).
- Switch on your terminal

Using your terminal

Please note: The screens-shots and receipt examples on your terminal may differ in detail from those depicted in this manual.

Turning the terminal on

Connect power supply to a nearby electrical outlet. Hold down the power button (located above the red cancel X button) until the display illuminates. Remove the protective film from the display if present.



Welcome screen

Turning the terminal off

To turn the terminal off press the power button for three seconds, ensure **'SHUTDOWN'** is highlighted and press the green **'OK'** key.

Please note: Highlighting **'RE-START'** will re-start the payment application.

Using your terminal (cont.)

Terminal keypad

The V3M2 Wi-Fi, V3M2 GPRS and V3C all share a common keypad layout (although the key layout may vary)

- The **'MAIN MENU'** key represented by a F1 Key and positioned above the **'1'** key toggles between menus.
- The 'F2', 'F3' and the 'F4' keys are allowing to access various options within 'Sale Application' menu
- The 'ARROW' keys are used to move to the next and previous menu screens. When activated, an arrow will also be seen on the display above the appropriate key.
- The numeric keys.

Keypad

The **'#'** key allows the cycling of character selection on the numeric keys during text entry. For example pressing **'1'** and then **'#', '#', '#'** will cycle through **1, Q, Z, 1.**

The star key is used to cycle through the following nine characters: **. , / @ * # ( )** – during text entry.

The action of the green **OK** key will be displayed in a **green** box at the bottom of the display.

The action of the red **X** key will be displayed in a **red** box at the bottom of the display.

The action of the yellow key will be displayed in a **yellow** box at the bottom of the display.

The green **ENTER** key will select **YES.**

The yellow **CLEAR** key will select **NO.**

Using your terminal (cont.)

Terminal display

The Vega 3000 products all share common graphical display. The display is separated into three specific areas:

Status bar

At the top of the display is a black bar with white text and coloured icons. This is known as the status bar and displays the folowing information from the left:

- Battery level indicator (only portable terminals). See 'Icon index' section for details.
- Date in dd/mm/yy format.
- Time in hh:mm format.
- Connection method icon. See icon index.
- Signal (GPRS or Wi-Fi) strength icon (V3M2 GPRS and V3M2 portable terminal only). See icon index.

Middle of screen

The middle of the screen (largest area) is used to display choices for data entry requests, instructions, transaction progress and any other relevant information.

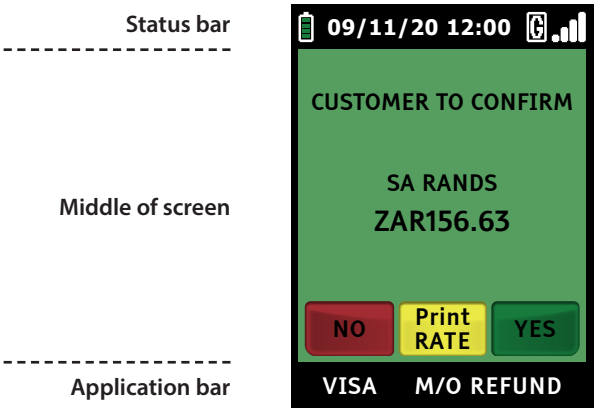
To represent specific operating modes, this part of the displays different colour backgrounds:

- Green: Transaction flow screens
- Blue: Reports and menus

Application bar

At the bottom of the screen there is a black bar with white text. This is known as the application bar and it displays information about the transaction in progress.

Using your terminal (cont.)



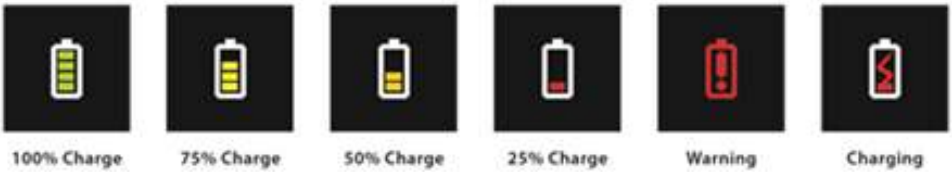
Screen saver

If a key has not been pressed for 30 seconds, the terminal's display will automatically revert to a screen saver. This will be displayed for a further 3 minutes, after which the display will go blank (V3M2 Wi-Fi and V3M2 GPRS). Pressing any key will turn the display back on.

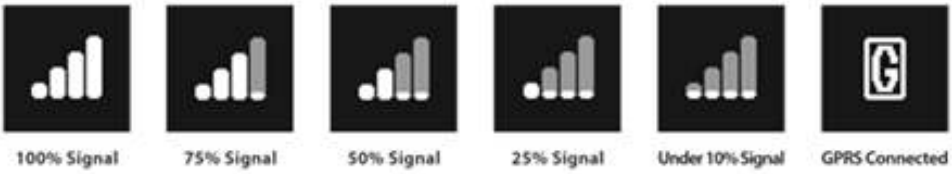
Icons index

The following is an index to the icons shown in the status bar:

Battery level indicator



Signal strength indicator



Connectivity indicators

Icons index (cont.)

The following is an index to the miscellaneous icons

Additional icons

SHIFT Engaged

Numbers

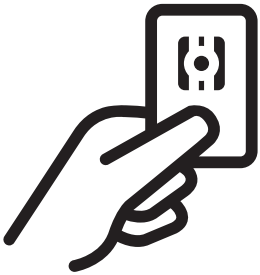
Lowercase

Uppercase

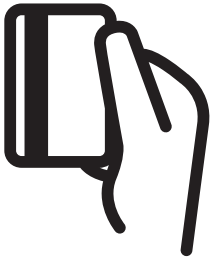
Welcome screen graphics

Screen buttons

Contactless icon



Chip & Pin icon

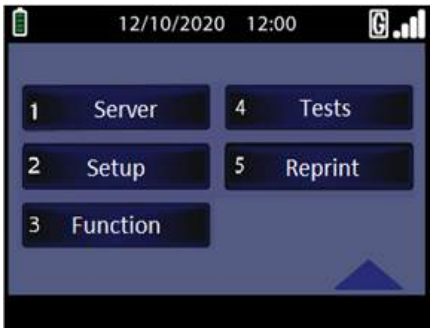


Swipe Card icon

Menu operation

Reports and terminal menu

The screens below show the Reports and Terminal Menu. This is displayed by pressing the F1 key when the Transaction Menu or Welcome Screen is displayed. The menu options may be split between two screens. To access the second screen, press the **ARROW** key below the display. This operation can be repeated from the second screen to return to the first part of the menu..



Selection of an item from a menu can display a sub-menu with more options (see right for an example). You may return to the original menu by pressing the '**UP**' arrow key.

Training mode

Please note: The Training Payment Card is not supplied with the terminal as standard.

Once the terminal is switched to Training Mode it enables the user to perform all transaction types without the actual transfer of funds. You may use normal Chip and PIN cards to perform these training transactions.

How to switch to Training Mode
Ensure the terminal is displaying the Welcome screen.

- Press the 'F1' key to display the Transaction Menu.
- Select 'TERMINAL' from the menu.
- Select 'TRAINING' from the menu.
- Type in the local password (default is 0000) and press the green 'OK' key.
- The screen will display 'SWITCH TO TRAIN MODE'.
- Select 'YES' by pressing the green 'OK' key.
- Press the 'F1' key to return to the Welcome screen.

Using Training Mode

Once in Training Mode, the text '**TRAINING MODE**' will be printed on all receipts. Depending on the amount entered, the simulated response will be different, allowing staff to simulate all transaction outcomes. Use the Training Payment Card to start a transaction.

- 0.01 to 100 (£0.01 to £1.00 or €0.01 to €1.00 in ROI) will display **AUTH CODE XXXX.**
- 200 (£2.00 or €2.00 in ROI) will display **REJECTED.**
- 300 (£3.00 or €3.00 in ROI) will display **DECLINED BY CARD.**
- 400 (£4.00 or €4.00 in ROI) will display **PICK UP CARD.**
- Any other amount will display **INVALID AMOUNT.**
- If you are prompted for a cardholder PIN, use **1234.**

Training mode (cont.)

How to leave Training Mode

Ensure the terminal is displaying the Welcome screen.

- Press the 'F1' key to display the Reports and Terminal Menu.
- Select 'TERMINAL' from the menu.
- Select 'TRAINING' from the menu.
- Type in the local password (default is 0000) and press the green 'OK' key.
- The screen will display 'LEAVE TRAINING MODE'.
- Select 'YES' by pressing the green 'ENTER' key
- Press the 'F1' key to return to the Welcome screen.

Please note: Ensure you do not attempt live transactions in Training Mode as the funds will not be transferred into your bank account.

Setting the merchant password

You may be asked to enter a password to perform certain functions. Different passwords protect different terminal functions and it is best to change these from the factory default to protect against potential fraudulent usage of the terminal. We stronlgly reccomend to change this password on a regular basis.

Please note: To protect against fraudulent activity with regard to voice referred transactions, you must amend your merchant password to your own value.

Local (merchant) password

The local password (sometimes referred to as a merchant password) is used to protect certain terminal functions, such as the End of Day Settlement process and Refunds. This password comprises of four digits and has a factory default of 0000. If you forget this password, please contact your helpdesk. To change the local password follow the procedure below:

- Ensure the terminal is displaying the Welcome screen.
- Press the 'F1' key to display the Reports and Terminal Menu.
- Press the down 'ARROW' key to show the additional menu items.
- Select 'SETUP' from the menu.
- Select 'PASSWORD' from the menu.
- Select 'CHANGE' from the menu.
- Type in the old password and press the green 'OK' key.
- Type in the new local password (default is 0000) and press the green 'OK' key.
- Repeat the previous step.
- The terminal will beep and display 'TRANSACTION ACCEPTED'.

The local password is now updated.

Maintenance password

The maintenance password is used to protect supervisory terminal functions. This password comprises of six digits. You will to need call your helpdesk to obtain this password.

Page 34

Transactions

Your terminal is able to provide the following transaction types:

- Sale
- Sale with Cashback
- Sale with Tip
- Pre-Authorisation
- Completion
- Refund

Please note: By default, your terminal will not be configured to accept all transaction types. Please contact your terminal leasing company for further details on how to add other transactions.

Please note: There are multiple configurable options on the Vega 3000 range of terminals which are set by the acquirers. As such the transaction flows within this manual may vary slightly to those displayed on your terminal.

How to insert a chip card

If your terminal is fitted with a PIN Pad, the card reader in the terminal is disabled. In this situation the cardholder inserts his/her Chip Card into the PIN Pad card reader. If no PIN Pad is fitted, the cardholder can insert his/her Chip Card into the terminal or, if preferred, they can ask you to perform the operation.

How to insert a chip card

If the card has a Chip on the front, insert the card either in the main terminal or separate PIN Pad (SPp10) with the Chip facing up and towards the terminal/PIN Pad. When the card is inserted correctly you should feel some resistance and hear an audible soft 'click'.

Transactions (cont.)

How to swipe a card

If the card presented is a Chip Card, it must be inserted into the terminal. If your terminal cannot read the Chip you may be given the option to swipe the card's magnetic stripe. As an additional security measure you may be requested to enter the last 4 digits of the card number.
If a Chip Card is swiped prior to being inserted into the terminal, the terminal will request the card is inserted into the Chip Card reader.
Swipe the card with the magnetic stripe facing down and towards the terminal. Swipe the card quickly in either direction.

Presenting a contactless card

Presenting a contactless card

Most card types support contactless technology. This is the ability for a payment to be taken by simply holding the card in close proximity (a few millimetres) to the terminal. This is known as 'presenting' the card. This method of payment is for small transactions and is designed to speed up the entire process. Contactless technology is available as standard on the Vega 3000 terminal family.

How to present a contactless card

The card must be placed close to the display area (within few milimeters for several seconds during which time the LEDs will indicate the read status (see LED status table below)

Contactless limits

You will be prompted to perform a Chip and PIN or Swipe transaction if the amount entered is not suitable for completion as a Contactless transaction.

Please refer to your Acquirer for further details.

Cardholder authentication

A contactless transaction will neither prompt for the cardholder's PIN nor signature. However, depending on previous contactless use on the card, it may prompt the terminal to revert to a Chip and PIN transaction for security purposes.

Contactless transactions supported

The following transactions are permissible with a contactless card:

- Sale
- Refund

If a transaction type not listed above is requested by a contactless card, the terminal will prompt for a Chip and PIN (or Swipe transaction.

Receipts

A merchant receipt is printed with every contactless transaction, but the printing of a customer receipt is optional. The skipping of this step speeds up the transaction process further.

Presenting a contactless card (cont.)

Card reading status

Four LEDs are present above the display, providing feedback on the success of the operation.

Contactless status	LED 1	LED 2	LED 3	LED 4
NOT READY The reader is not ready to read a card. This can be caused by lack of power or failure in communicating with the terminal.	OFF 	OFF 	OFF 	OFF 
IDLE The reader has power, but is waiting for information from the terminal before being able to read contactless cards.	BLINKING 	OFF 	OFF 	OFF 
READY TO READ CARD The reader is ready to start the transaction and can read contactless cards.	ON 	OFF 	OFF 	OFF 
CARD READ SUCCESSFULLY STAGE 1 This indicates the first stage of card reading has been successful.	ON 	ON 	OFF 	OFF 
CARD READ SUCCESSFULLY STAGE 2 This indicates the second stage of card reading has been successful.	ON 	ON 	ON 	OFF 
CARD READ SUCCESSFULLY STAGE 3 This indicates the third stage of card reading has been successful.	OFF 	OFF 	OFF 	OFF 
CARD READ SUCCESSFULLY STAGE 4 All lights will turn off within a quarter of a second. This means the cardholder may remove their card.	OFF 	OFF 	OFF 	OFF 
CONTACTLESS CARD READING HAS NOT BEEN SATISFIED POSSIBLY CAUSED BY A problem with the contactless read process. The reason for this error will be displayed. The process has not satisfied all the criteria and the cardholder will be asked to insert the card in the chip reader to perform the transaction.	OFF 	OFF 	OFF 	OFF 

Typing in card numbers

Customer present

If the terminal cannot read the Chip or the magnetic stripe on the card, you can type in the long number on the front of the card. Once all the information has been entered and the transaction approved by the acquirer the terminal will ask for the cardholder to sign the merchant's copy of the receipt.

Please note: Signature verification is not as secure as Chip and PIN and you may incur charge-backs from your acquirer if you use it.

Customer not present

If the cardholder is not present (e.g. a mail order customer) you can also type in the long number on the front of the card.

If you select '**CANCEL**' by pressing the yellow 'Arrow'' key when the terminal asks whether the cardholder is present, you may be asked to type in the 3-digit CVV2 code and address details. A response will be given, at which point you can choose to accept or cancel the transaction. (See Appendix A for transaction responses.)

Please note: American Express Customer not present transactions will require entry of a 4-digit CVV2 code.

Typing in amounts

When you or the cardholder are requested to enter an amount, it is entered in pence (or cents in ROI). Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

If a mistake is made, press the yellow 'ARROW' key to delete the last number entered.

Typing in other data

If a mistake is made entering any other data such as card number, expiry date, authorisation code, etc., the entire field can be deleted by pressing the yellow 'ARROW' key once.

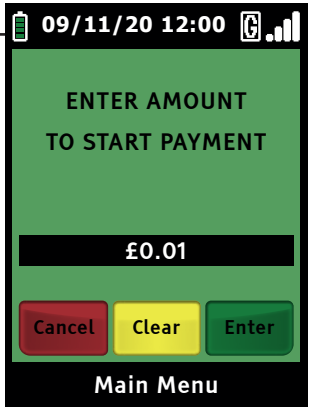
Please note: Pressing the yellow 'ARROW' key twice will cancel the transaction.

Sale – Inserting a chip card

Step 1

When the terminal is ready to perform a Sale transaction it will show the 'Enter amount ' screen. You can start a Chip and PIN Sale transaction in one of two ways:

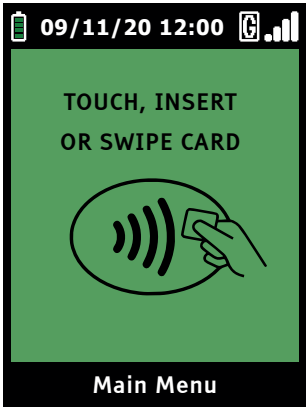
Option 1



Enter the Sale amount in pence (or cents in ROI) and press the green '**OK**' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow '**ARROW**' key.



Insert the Chip Card into the terminal's Chip Card reader

Sale – Inserting a chip card (cont.)

Option 2

Insert the Chip Card into the terminal's Chip Card reader. A Sale transaction will be initiated. Type in the Sale amount in pence (or Cents for ROI) and press green 'OK' key.

Example:
Type in the Sale amount in pence (or cents for ROI) and press the green 'OK'
Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the entire field can be deleted by pressing the yellow 'ARROW' key once.

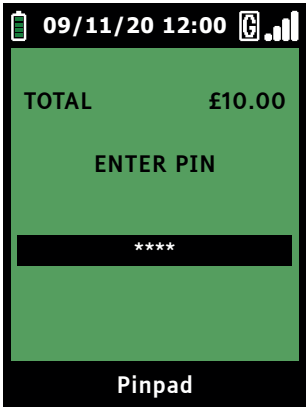
Step 2

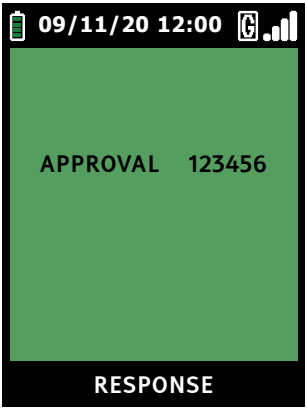
The cardholder must type in his/her PIN (Personal Identification Number) on the terminal's keypad. After the PIN has been entered, the cardholder should press the green 'ENTER' key on the PIN entry device.

The terminal will now connect to your acquirer and display progress.

If the transaction is approved, the Approval Code will be displayed and the terminal will print the merchant's copy of the receipt.

(See Appendix A for possible transaction responses.)





Sale – Inserting a chip card (cont.)

Step 3

Remove the card.

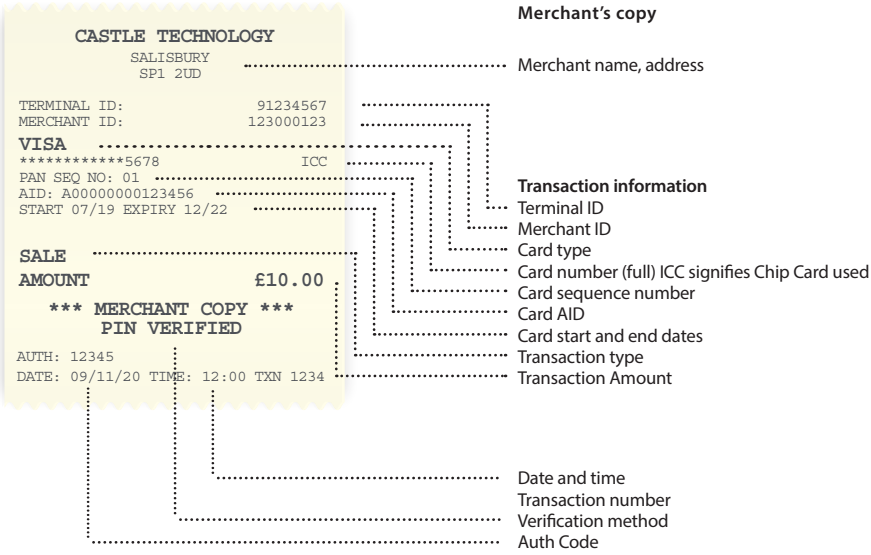
Step 4

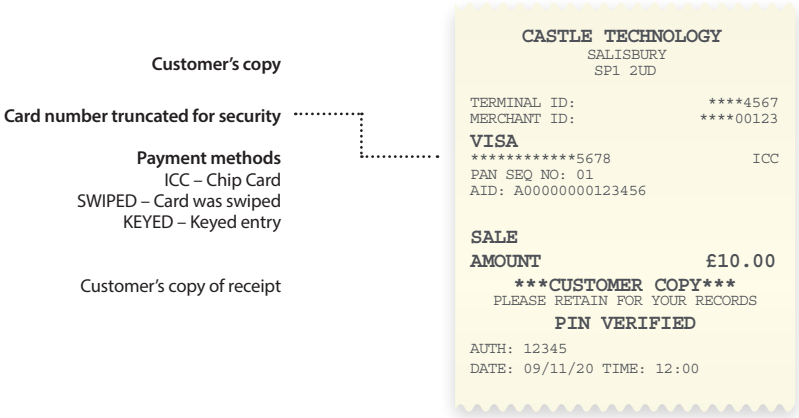
The terminal will then print the merchant's copy of the receipt. Then press the green '**OK**' key.

Step 5

The terminal will then print the customers copy of the receipt. Hand this receipt to the card holder and return their card. The transaction is now complete. The terminal will automatically return to the Welcome screen.

Example of sale receipts





Sale – Swiping a card

If your terminal cannot read the Chip on the presented Chip Card (or one is not present) you may be given the option to swipe the card's magnetic stripe (located on the rear of the card).

Step 1

When the terminal is ready to perform a Sale transaction it will show the Welcome screen.

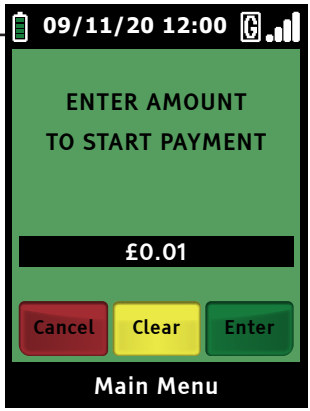
You can start a Sale transaction in one of two ways:

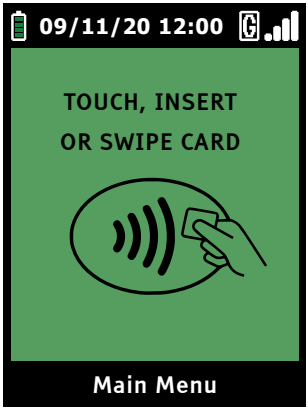
Option 1

Enter the Sale amount in pence (or cents in ROI) and press the green 'OK' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow 'ARROW' key.





Swipe the card in the terminal's magnetic stripe reader (see Transactions (cont.) on page 35).

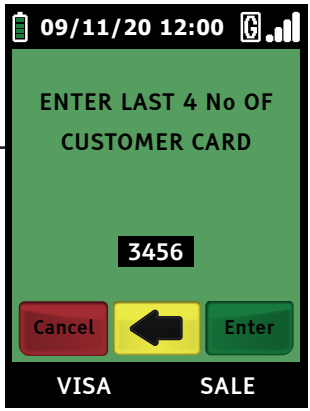
Sale – Swiping a card (cont.)

Option 2

Swipe the Card in the terminal's magnetic stripe reader (see page 35). A Sale transaction will be initiated. Type in the Sale amount in pence (or cents for ROI) and press green 'OK' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow '**ARROW**' key.



Step 2

You may be asked to enter the last 4 digits of the card number for an additional security check. Enter the four digits and press the green '**OK**' key.

The terminal will display the card type.

Step 3

The terminal will now connect to your acquirer and display progress.

Once complete, the terminal will print the merchant's copy of the receipt.

Tear off the receipt and press the green '**OK**' key. Ask the cardholder to sign on the dotted line.

Sale – Swiping a card (cont.)

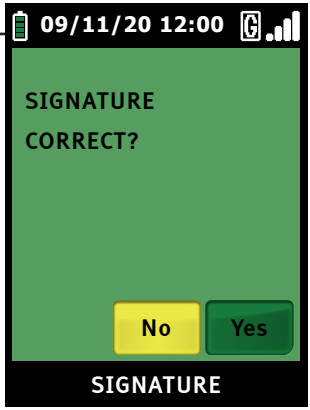
Step 4

Compare the cardholder's signature on the receipt to that on the rear of the card.

If you are happy with the signature comparison, select '**YES**' by pressing the green '**OK**' key. The transaction will be approved and a customer copy of the receipt will be printed. Go to step 5.

If you are not happy with the signature, select '**NO**' by pressing the yellow '**ARROW**' key.

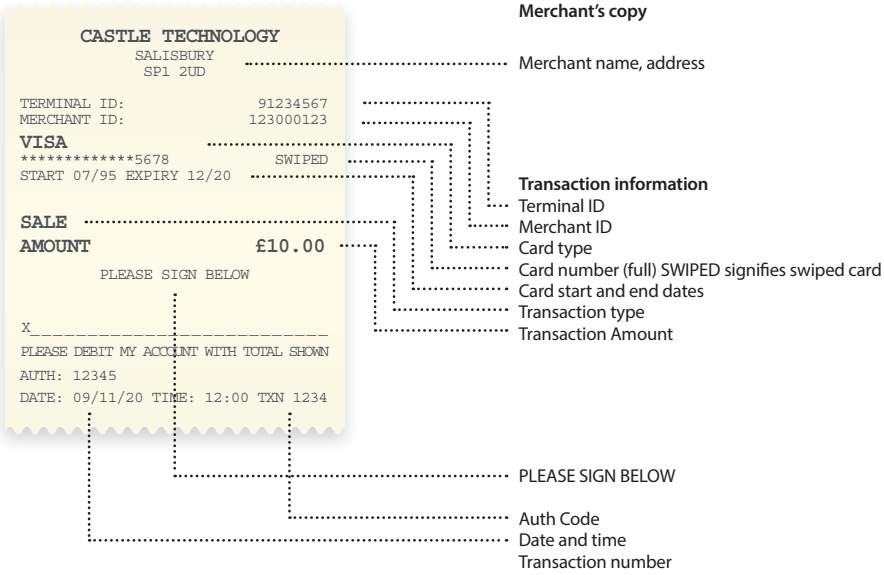
The terminal will print a merchant reversal receipt for the origi-nal transaction amount. Tear off and keep for your records. Press the green '**OK**' key.

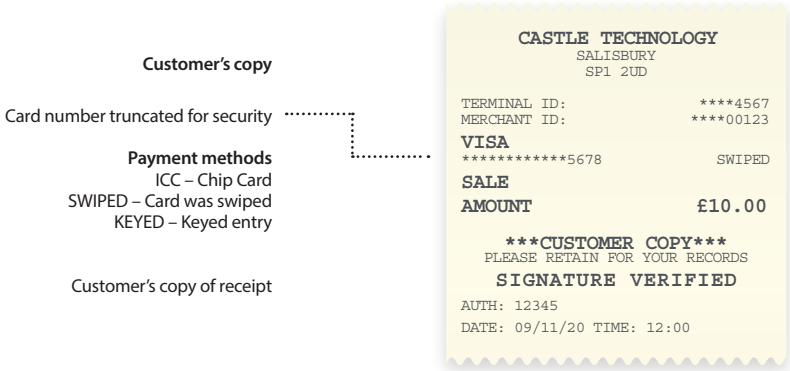


Step 5

Tear off the customer's copy and hand it to the cardholder along with his/her card. The transaction is now complete. The terminal will automatically return to the Transaction Menu.

Example of sale receipts (swiped card)





Sale – Presenting a contactless card

The terminal will offer contactless payment if:

- the terminal supports the functionality;
- the card supports the functionality;
- and the transaction amount is suitable.

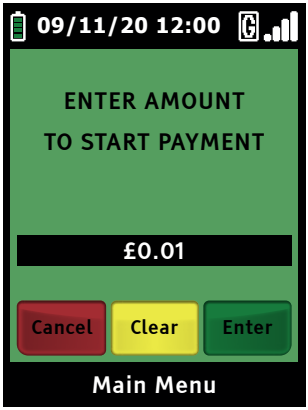
Step 1

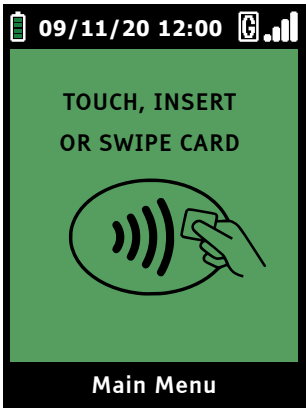
When the terminal is ready to perform a Sale transaction it will show the 'Enter amount screen.

If the cardholder requests a contactless payment you must first enter the Sale amount in pence (or cents in ROI) and press the green '**OK**' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow '**ARROW**' key.

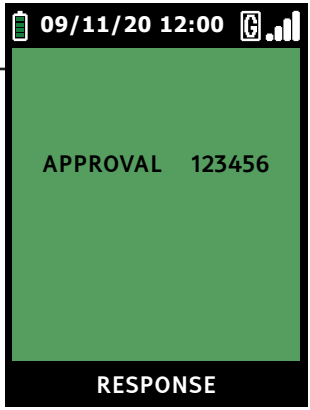




Ask the customer to place his/her card in close proximity to the terminal display. The four LEDs at the top of the display will indicate a successful read (see page 37).

Once the card i s successfully read, ask the cardholder to remove the card.

Sale – Presenting a contactless card (cont.)



Step 2

The terminal will now connect to your acquirer and display progress.

If the transaction is approved, the Approval Code will be displayed terminal will print the merchant's copy of the receipt.

(See Appendix A for possible transaction responses).

Step 3

The merchant's copy of the receipt will be printed.

Step 4

The terminal will automatically return to the 'ENTER AMOUNT' screen.

Step 5

If a customer requests a receipt, please refer to page page 70 of this user manual.

Example of sale receipts (presented contactless card)

The receipt is identical to the Chip Card Sale receipt, except '**CONTACT**' replaces '**ICC**', and '**VERIFIED BY PIN**' is replaced by 'Cardholder not veryfied'.

Sale and cashback (inserting a chip card)

This is similar to a regular Sale transaction and, if enabled, replaces the standard Sale transaction described previously. There is a facility to enter an additional figure for Cashback.

Please note: This is a service that must be requested from your acquirer. Cashback is only allowed on Debit Cards, not Credit Cards.

Step 1

When the terminal is ready to perform a Sale and Cashback transaction it will show the Enter amount screen.

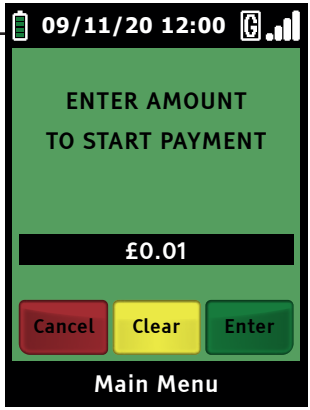
You can start a Chip and PIN Sale and Cashback transaction in one of two ways:

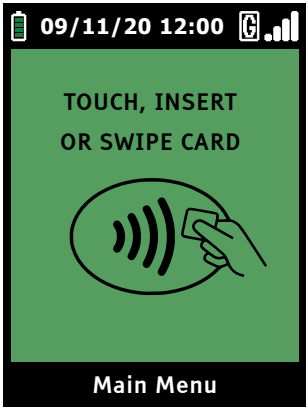
Option 1

Enter the Sale amount in pence (or cents in ROI) and press the green '**OK**' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow '**ARROW**' key.





This screen will be displayed

Sale and cashback (cont.)

Insert the Chip Card into the terminal's Chip Card reader

Option 2

Insert the Chip Card into the terminal's Chip Card reader. Type in the Sale amount in pence (or cents for ROI) and press the green '**OK**' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow '**ARROW**' key.

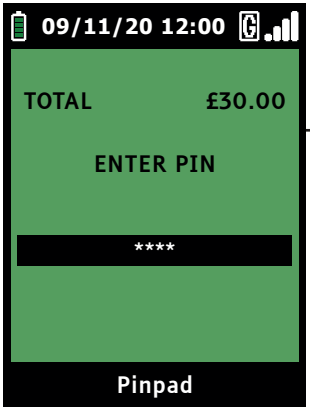
Step 2

Type in the Cash amount. and press the green 'OK' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

If no cash back is required, press green 'OK' key without typing any amount.

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow '**ARROW**' key.

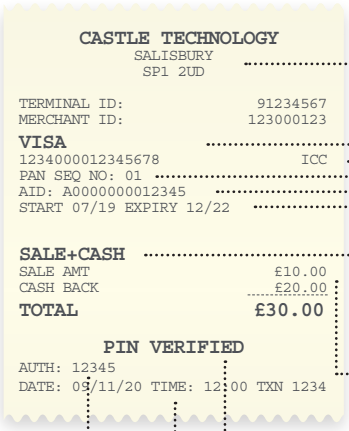


Step 3

You may be asked to confirm the amount, after which the cardholder must type in his/her PIN (Personal Identification Number) on the terminal keypad . After the PIN has been entered, the cardholder should press the green '**OK**' key.

The terminal will now attempt to connect to your acquirer and the rest of the transaction will continue in the same way as for a normal Chip and PIN sale.

Example of sale and cashback receipts



CASTLE TECHNOLOGY
SALISBURY
SP1 2UD

TERMINAL ID: 91234567
MERCHANT ID: 123000123

VISA
1234000012345678 ICC
PAN SEQ NO: 01
AID: A0000000012345
START 07/19 EXPIRY 12/22

SALE+CASH
SALE AMT £10.00
CASH BACK £20.00
TOTAL £30.00

PIN VERIFIED
AUTH: 12345
DATE: 09/11/20 TIME: 12:00 TXN 1234

Merchant's copy

Merchant name, address

Transaction information
Terminal ID
Merchant ID
Card type
Card number (full) ICC signifies Chip Card used
Card sequence number
Card AID
Card start and end dates
Transaction type
Transaction Amount & Cashback Amount

Verification method

Date and time
Transaction number

Auth Code

Customer's copy

Card number truncated for security

Payment methods
ICC – Chip Card
SWIPED – Card was swiped
KEYED – Keyed entry

Customer's copy of receipt

CASTLE TECHNOLOGY
SALISBURY
SP1 2UD

TERMINAL ID: ****4567
MERCHANT ID: ****00123

VISA
**********5678 ICC
PAN SEQ NO: 01
AID: A0000000012345

SALE+CASH
SALE AMT £10.00
CASH BACK £20.00
TOTAL £30.00

CUSTOMER COPY
PLEASE RETAIN FOR YOUR RECORDS
PIN VERIFIED
AUTH: 12345
DATE: 09/11/20 TIME: 12:00

Sale and tip – Inserting a chip card

This is much the same as a regular Sale transaction but with the added ability of including a tip in addition to the transaction amount.

Please note: This is a service that must be requested from your acquirer. When activated, tipping will be set by default for all Sale transactions.

Step 1

When the terminal is ready to perform a Sale and Tip transaction it will display the Welcome screen.

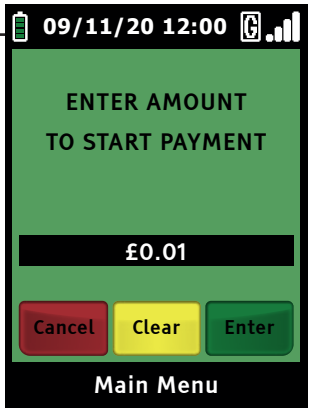
You can start a Chip and PIN Sale and Tip transaction in one of two ways:

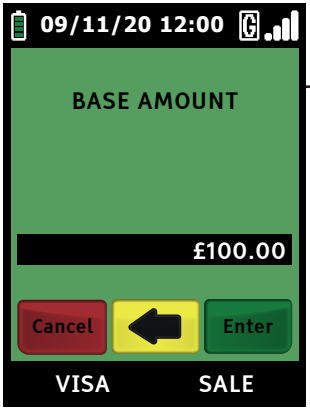
Option 1

Enter the Sale amount in pence (or cents in ROI) and press the green 'OK' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow 'ARROW' key.





Option 2

Insert the Chip Card into the terminal's Chip Card reader. Type in the base amount in pence (or cents for ROI) and press the green 'OK' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

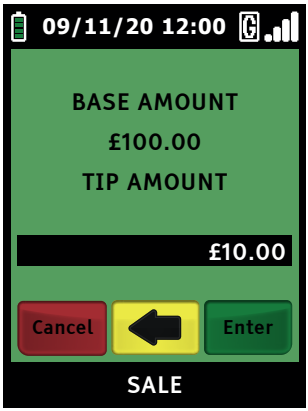
Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow 'ARROW' key.

Sale and tip – Inserting a chip card (cont.)

Step 2

Ask the cardholder if they wish to enter a tip. If the answer is yes, select '**YES**' by pressing the green '**OK**' key. If the answer is no, select '**NO**' by pressing the red '**X**' key.

If the cardholder chooses '**YES**' by pressing the green '**OK**' key. Type in the base amount in pence (or cents for ROI) and press the green 'OK' key.



Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the last digit can be deleted by pressing the yellow 'ARROW' key.

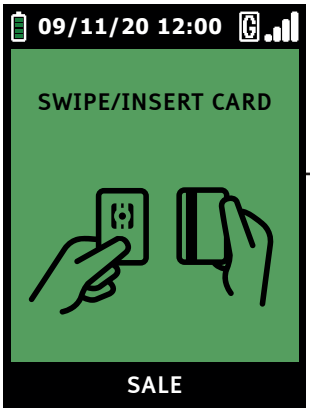
Step 3

The cardholder is requested to confirm the tip amount.

Sale and tip – Inserting a chip card (cont.)

Step 4

The cardholder should confirm the total value of the transaction, by selecting '**YES**' by pressing the green '**OK**' key'.



Step 5

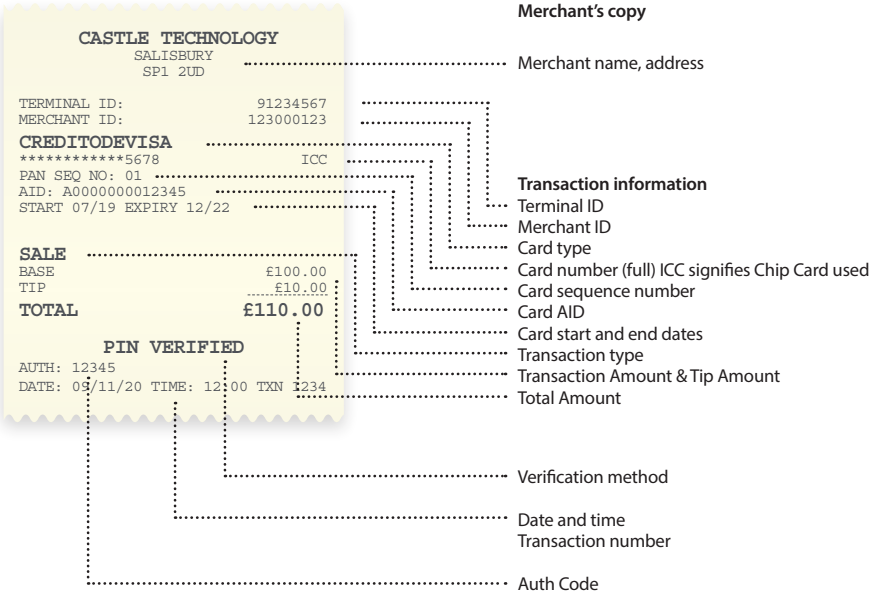
If the transaction was started by inserting or swiping the card (Option 2), then go to Step 6. Otherwise you will be requested to insert or swipe the card.

Insert the Chip Card into the terminal's Chip Card reader.

Step 6

The cardholder will be prompted for his/her PIN on the terminal. After the PIN has been entered, the cardholder should press the green 'OK' key. The terminal will now attempt to connect to your acquirer and the rest of the transaction will continue in the same way as for a normal Chip and PIN sale.

Example of sale and tip receipts



Customer's copy

Card number truncated for security

Payment methods
ICC – Chip Card
SWIPED – Card was swiped
KEYED – Keyed entry

Customer's copy of receipt

Hotel and rental operations

The Vega 3000 family of terminals allow transaction types for use in the hotel industry. These transaction types are also relevant for other merchant categories such as car rentals.

The transaction is performed in two parts: a 'Pre-Authorisation' and a confirming 'Completion'.

Hotel and Rental configuration, Express Check-Out feature (that allows Customer Not Present check-out) and Tipping features are not available unless requested and agreed with your bank.

Pre-authorisation – Check-in

The Pre-Authorisation is performed during check-in. The final bill is estimated and the cardholder's account checked for sufficient funds. The estimated amount is reserved in, but not taken from, his/her bank. The funds are eventually taken using a Completion transaction when the cardholder settles his/her bill on check-out. There are, of course, other situations where these transactions would be useful.

A Pre-Authorisation transaction must be completed within a set amount of time. If not completed within this period it will become invalid and reallocated funds will return to the cardholder's account. Your bank can advise you on this time limit.

The value of the Completion must also be within a specified range of the original Pre-Authorisation (not dramatically different). Your bank can advise on the upper and lower variances allowable.

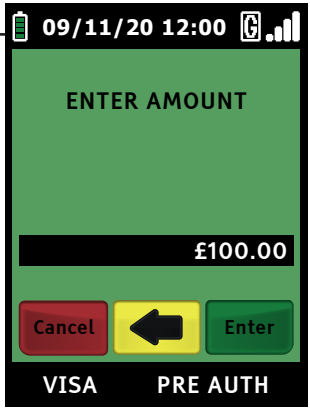
Step 1

Select the '**PRE-AUTH**' transaction type from either the Transaction Menu or the '**TRANS**' option of the Terminal and Reports Menu. The exact location will be dependent on your terminal's configuration.

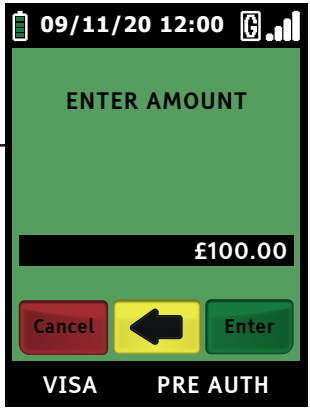
Type in the Pre-Authorisation amount in pence (or cents for ROI) and press the green '**OK**' key.

Example: Typing in 10000 would equate to a value of £100.00 (€100.00 in ROI).

Please note: If a mistake is made entering data, the last digit can be deleted by pressing the yellow '**ARROW**' key.



Hotel and rental operations (cont.)



Step 2

The terminal will prompt for the cardholder's card to be inserted or swiped. The transaction will continue in the same way as a normal Chip and PIN Sale.

Merchant's copy

Auth Code

CASTLE TECHNOLOGY
SALISBURY
SP1 2UD

TERMINAL ID: 91234567
MERCHANT ID: 123000123
CREDITODEVISA
1234000012345678 ICC
PAN SEQ NO: 01
AID: A0000000012345
START 07/17 EXPIRY 07/21

AUTHORISATION ONLY
AMOUNT £100.00

PIN VERIFIED
AUTH: 12345
DATE: 09/11/20 TIME: 12:00 TXN 1234

IMPORTANT:
The merchant receipt must be kept in a safe place as you will need to refer to the 'AUTH' number when performing the Completion transaction.

If the estimated amount used for the Pre-Authorisation is no longer adequate to cover the estimated final bill, incremental authorisation should be performed, e.g. for an extended stay. This may be required if the Pre-Authorisation expires (your bank must advise on how long Pre-Authorisations remain valid). An incremental Pre-Authorisation is performed in exactly the same way as a Pre-Authorisation above.

Completion – Check-out

A Completion transaction is performed at the end of a stay to debit funds from the card holder. For a rental environment, this will be when the vehicle is returned. In order to perform a Completion transaction, a Pre-Authorisation must have been previously performed using the same card. You will need the authorisation code from the most recent Pre-Authorisation receipt relating to this transaction. You do not need to use the same payment terminal as was used for the Pre-Authorisation.

Step 1

Select the '**Completion**' transaction type from either the Transaction Menu or the '**TRANS**' option of the Terminal and Reports Menu. The exact location will be dependent on your terminal's configuration.

Insert the Chip Card into the terminal's Chip Card reader or PIN Pad (if fitted)

OR

Type in the card number. If the card number is keyed the terminal will prompt '**Customer Present**'. For an Express Check-Out select '**NO**' by pressing the red '**CANCEL**' key, otherwise select '**YES**' by pressing the green '**ENTER**' key.

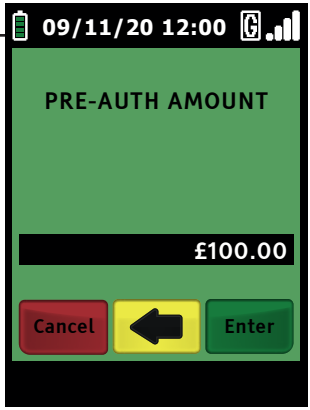
Step 2

Type in the Pre-Authorisation amount in pence (or cents for ROI) and press the green '**OK**' key.

If you performed incremental Pre-Authorisations, then you must enter the total value of all Pre-Authorisations on this card.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow '**ARROW**' key.



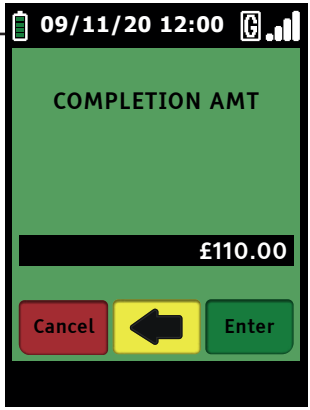
Completion – Check-out (cont.)

Step 3

Type in the Completion amount in pence (or cents for ROI) and press the green '**OK**' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the last digit can be deleted by pressing the yellow '**ARROW**' key.



Step 4

Completion amount confirmation is requested by pressing the green '**OK**' key.

Step 5

Refer to the receipt for the latest Pre-Authorisation on this card and note the '**AUTH**' code printed near the bottom. Key this '**AUTH**' code and press the green '**ENTER**' key. The terminal will now connect to your acquirer and display progress.

If the transaction is approved, the Approval Code will then be displayed and the terminal will print the merchant's copy of the receipt.

(See Appendix A for possible transaction responses.)

Completion – Check-out (cont.)

Step 6

Remove the card and the merchant's copy of the receipt and press the green 'ENTER' key. The terminal will then print the customer's copy of the receipt.

Step 7

Tear off the customer's copy and hand it to the cardholder. For an Express Check Out or No-Show, you must mail this to the cardholder.

Express Check-out

Express Check-Out is performed in the same way as a normal Completion transaction documented above, selecting No at the Customer Present prompt.

Note: You will require agreement from your leasing company to perform Express Check-Out transactions.

Additional Charge after Check-Out and No-Show

Any additional charges identified after Check-Out or charges arising from a No-Show situation should be processed as separate card not present Sale transactions.

Tipping

It is possible to activate tipping at Check-Out. In this case the terminal will prompt for a Base Amount then a Tip Amount before confirming the transaction. Please contact your leasing company if you require the tipping feature. An example transaction is as follows:

A hotel charges £100 per night for a room. A customer arrives at the hotel and indicates that they will be staying for five nights. A Pre-Authorisation is performed for £500.

Before checkout the customer indicates that they will be staying for an additional two nights. Because this is a significant portion of the original bill the hotel chooses to perform a top-up authorisation. This is for £200 for the extra two nights.

Whilst at the hotel the customer spends £10 in the bar each night bringing the total bill to £770.

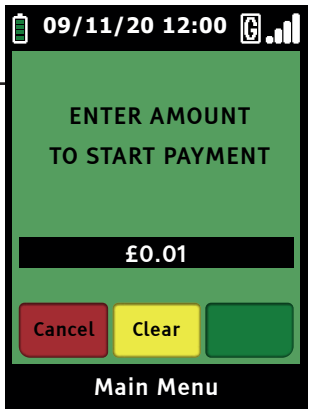
The Completion transaction is performed with the Pre-Authorisation amount of £700 (the sum total of the previous authorisations) and the authorisation code from the second Pre-Authorisation. The final amount entered for the transaction is £770.

Sale transaction – Customer not present (keyed)

This method is used for taking transactions when the cardholder is not next to the terminal – a telephone order, for example.

Please note: Some of the screens which ask for information are dependent on your terminal's configuration. If a screen is absent, simply skip to the next step.

Step 1



When the terminal is ready to perform a keyed Sale transaction it will show the Welcome screen. Enter the Sale amount in pence (or cents in ROI) and press the green '**OK**' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the last digit can be deleted by pressing the yellow '**ARROW**' key.

Step 2

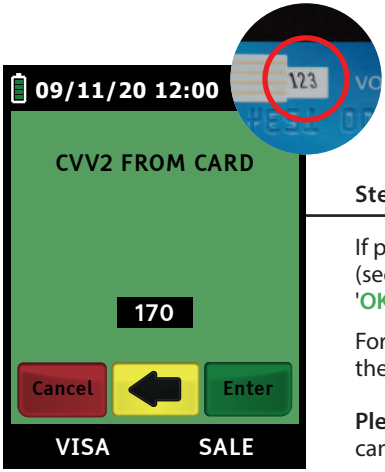
Carefully type in the long number on the front of the card. As you type you will notice the message changes from '**SWIPE/INSERT CARD**' to '**ENTER CARD NUMBER**', as the number begins to appear in the box on the screen. Once the number has been typed in correctly, press the green '**ENTER**' key. You may also be asked to enter the expiry date of the card.

Please note: If a mistake is made entering data, the the last digit can be deleted by pressing the yellow '**CLEAR**' key.

Sale transaction (cont.)

Step 3

Since the cardholder (and card) is not present, select '**NO**' by pressing the yellow '**ARROW**' key.

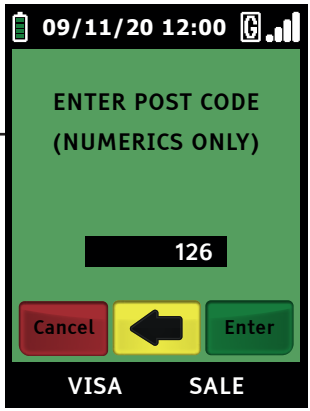


Step 4

If prompted, ask the cardholder for the 3 digit CVV2 code (security code) on the back of the card and press the green '**OK**' key.

For an American Express card enter the 4 digit code printed on the front of the card.

Please note: If a mistake is made entering data, the last digit can be deleted by pressing the yellow '**ARRROW**' key.



Step 5

If prompted, enter the number contained within the cardholder's postcode and press the green '**OK**' key.

Example: If the customer's postcode is SP12 6UD, enter '126'.

Please note: If a mistake is made entering data, the last digit can be deleted by pressing the yellow '**ARROW**' key.

Sale transaction (cont.)

Step 6

If prompted enter the numbers from the cardholder's first line of his/her address and press the green '**OK**' key.

Example: If the first line of the customer's address is 159 Baker Street, enter '**159**'.

Please note: If a mistake is made entering data, the last digit can be deleted by pressing the yellow '**ARROW**' key.

The terminal will now connect to your acquirer. After the terminal connects, it will display the response from your acquirer.

Step 7

The transaction will now continue as with a normal Sale transaction, but the PIN entry phase will be skipped. You will receive a response from the acquirer informing you whether the address and post-code entered are correct. You must decide if you are happy to continue with the transaction.

If you select '**NO**' by pressing the yellow '**ARROW**' key the terminal will print out the Reversal copy of the receipt and connect to your acquirer to reverse the transaction. If you select '**YES**' by pressing the green '**OK**' key, the transaction will complete.

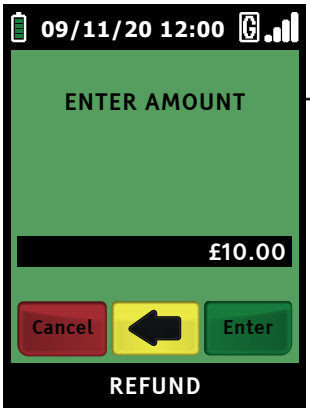
Example of sale receipt (Customer not present – keyed)

The receipts will have the same information as a swiped card, except the dotted line and declaration will be replaced by the text '**CUSTOMER NOT PRESENT**'.

Refund – Inserting a chip card

Step 1

Select the '**REFUND**' transaction type from either the Transaction Menu or the '**TRANS**' option of the Terminal and Reports Menu. The exact location will be dependent on your terminal's configuration.



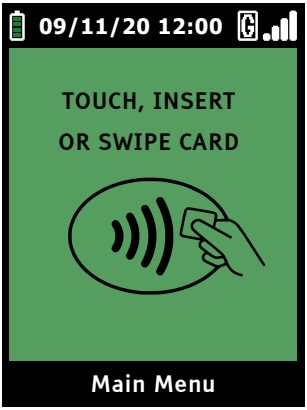
Step 2

Enter the Refund amount in pence (or cents in ROI) and press the green '**OK**' key.

Example: Typing in 1000 would equate to a value of £10.00 (€10.00 in ROI).

Please note: If a mistake is made entering data, the last digit can be deleted by pressing the yellow '**ARROW**' key.

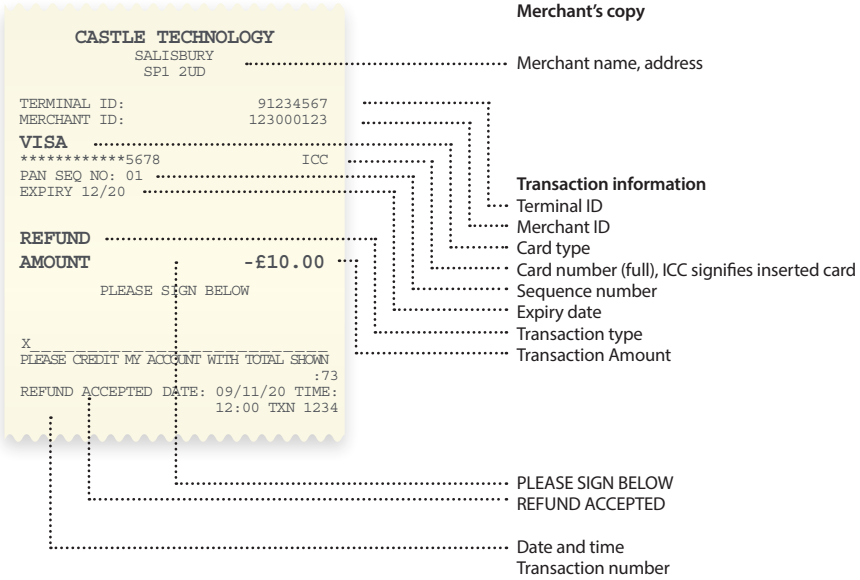
Insert the Chip Card into the terminal's Chip Card reader.

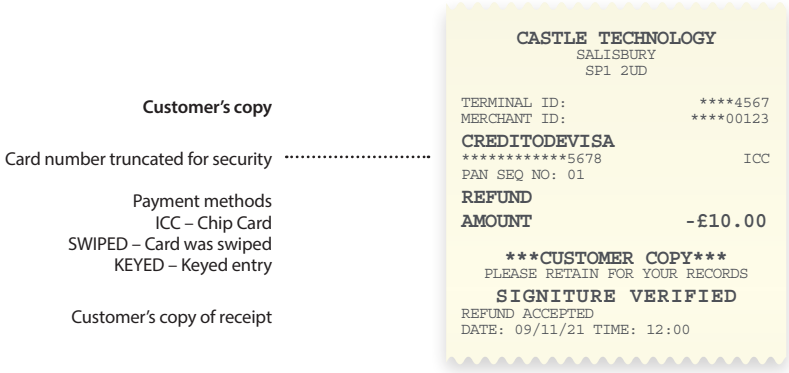


Step 3

The transaction will now complete as per a normal transaction, but the PIN entry phase will be skipped.

Example of refund receipt





Settlement

All Vega 3000 family terminals are configured to complete automatic end of day. To disable this feature please contact technical support.

For the totals to display correctly, this must be completed during the 'Banking Window' time set by your Acquirer. During a Settlement, the terminal will connect to your acquirer(s) and ensure that all transactions processed have been received.

Procedure

Step 1

Ensure the terminal is at the Welcome screen and press the 'MAIN MENU' key to display the Reports and Terminal Menu. Select 'BATCH' and then select 'SETTLE'.

Step 2

You may be requested to enter the Merchant Password.

Step 3

If your terminal is configured with multiple Acquirers, you can select the Acquirer you want to settle. However, the selection of 'ALL HOSTS' is recommended. The terminal will connect to the selected Acquirer(s) and print out the Settlement report. The Settlement totals will be reset to zero once this process is complete.

If you do not complete this procedure, it may result in your terminal failing to automatically update and may expose you to the risk of charge-backs.

Responses

Totals Agree / Balance Reconciled

Everything was received by your Acquirer(s) and the totals in the terminal match their totals.

Settlement (cont.)

Totals disagree / Out of Balance

There has been a discrepancy in the total value of the transactions that the Acquirer has and those in the terminal (i.e. the totals are out of balance).

The terminal will print the error code '73' on the receipt of each transaction after the discrepancy occurred. This will require you to review the receipt for that day's transactions to find the one that caused the error. Once discovered you can contact the Acquirer to rectify the situation.

Please note: Manual program updates will reset the totals and may cause this response.

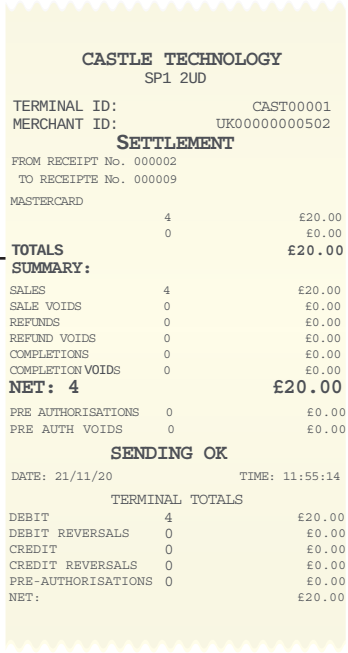
Totals unconfirmed

The terminal was unable to connect to your Acquirer(s) (See page 74 for help with troubleshooting communication problems or call the helpdesk).

Cannot confirm

The terminal was unable to connect to your Acquirer(s). This is only displayed when the terminal has previously attempted a Settlement that had a Totals Unconfirmed response.

Please note: If you are unsure of any aspect relating to the Settlement procedure, please contact your Acquirer or the helpdesk.



CASTLE TECHNOLOGY
SP1 2UD

TERMINAL ID: CAST00001
MERCHANT ID: UK00000000502

SETTLEMENT

FROM RECEIPT No. 000002
TO RECEIPTE No. 000009

MASTERCARD

	4	£20.00
	0	£0.00
TOTALS		£20.00

SUMMARY:

SALES	4	£20.00
SALE VOIDS	0	£0.00
REFUNDS	0	£0.00
REFUND VOIDS	0	£0.00
COMPLETIONS	0	£0.00
COMPLETION VOIDS	0	£0.00
NET: 4		£20.00
PRE AUTHORISATIONS	0	£0.00
PRE AUTH VOIDS	0	£0.00

SENDING OK

DATE: 21/11/20 TIME: 11:55:14

TERMINAL TOTALS

DEBIT	4	£20.00
DEBIT REVERSALS	0	£0.00
CREDIT	0	£0.00
CREDIT REVERSALS	0	£0.00
PRE-AUTHORISATIONS	0	£0.00
NET:		£20.00

Reports

There are a number of different reports available depending on your acquiring bank, each with a different purpose. To access the reports menu press the '**MAIN MENU**' button and select '**REPORTS**'.

Please note: The reports in this section are for optional usage and only designed to help you keep track of your orders and accounts. These reports are not a substitute for the Settlement procedure.

The Merchant password (default '0000') may be requested prior to running these reports. You maybe prompted to clarify the data you wish to view:

- Short/Limited: High level transaction summary
- Full: Detailed transaction report including individual transaction data.

Full View reports may not be available on your terminal.

Statement

This is a running report that can be printed off at any point in time during the day. It displays the total number and total value of transactions performed for each Acquirer since the last report was performed. This report DOES NOT reset the totals unless you select option to 'Reset statement' - this will reset the totals to '0'

```
09 NOV 20                    12:00
      STATEMENT REPORT
      CASTLES TECHNOLOGY
            SALISBURY
             SP1 2UD

TERMINAL ID:            91234567
.....................................
STREAMLINE
MERCHANT ID:            123000123

VISA
          2          £111.00 DR
          2           £20.00 CR
TOTAL               £91.00 DR
SUBTOTAL
FOR TXNS 0002-0011
          2          £111.00 DR
          2           £20.00 CR
TOTAL               £91.00 DR
.....................................
GRAND TOTALS
          2          £111.00 DR
          2           £20.00 CR
TOTAL               £91.00 DR
.....................................
TOTALS RESET
```

```
09 NOV 20                    12:00
      SATEMENT REPORT
      CASTLE TECHNOLOGY
            SALISBURY
             SP1 2UD

TERMINAL ID:            91234567
.....................................
STREAMLINE
MERCHANT ID:            123000123

VISA
          2          £111.00 DR
          2           £20.00 CR
TOTAL               £91.00 DR
SUBTOTAL
FOR TXNS 0002-0011
          2          £111.00 DR
          2           £20.00 CR
TOTAL               £91.00 DR
.....................................
GRAND TOTALS
          2          £111.00 DR
          2           £20.00 CR
TOTAL               £91.00 DR
.....................................
TOTALS NOT RESET
```

Short and full version

For Statement report you can print two versions:

Short - with total number of transactions

Full - with each transaction separated on the report

Reports (cont.)

Audit / Transaction Analysis

Performing an Audit on the terminal will print out a report of each transaction that has been put through the terminal since the last Settlement. This can be used in the unlikely event of a Settlement error, allowing you to check transactions in the terminal's batch against the Merchant copies of the receipts.

```
        SPIRE PAYMENTS
            SALISBURY
             SP1 2UD

TERMINAL ID:                 91234567
AUDIT REPORT              09 NOV 20
000001                    010003382
EVO Payments

INV# TRANS                      AUTH
CARD NUMBER                CARD TYPE
                                TOTAL

360464 SALE                     01024
************0010                 VIS
                               £1.00

360467 COMPLETION               00042
************0010                 VIS
                             £110.00

360472 REFUND                   10106
************0010                *VIS
                             -£10.00

360473 REFUND                   10114
************0010                *VIS
                             -£10.00
```

Short and full version

For Analysis report you can print two versions:

Short - with total number of transactions

Full - with each transaction separated on the report

```
        SPIRE PAYMENTS
            SALISBURY
             SP1 2UD

TERMINAL ID:            123000123456

TRANS TOTAL
BY ISSUER                 09 NOV 20

VISA
SALES      2                £111.00
REFUNDS    2                -£20.00
TOTAL      4                 £91.00
```

Saved EoD

Performing a Saved End of the Day report on the terminal will print out a copy of last successful batch report.

Reprint

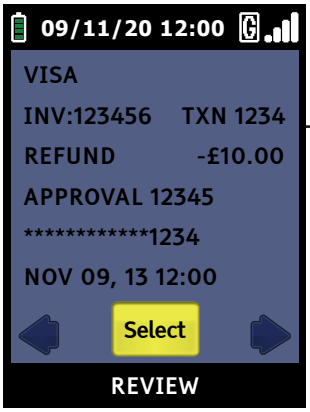
This allows you to quickly reprint a copy of the last transaction receipt.

Reviewing transactions/reprinting a receipt

The Vega3000 family of terminals maintain a Batch record of all transaction information since the last success-ful Settlement was performed. It is possible to review the Batch, find the appropriate transaction and, if required, reprint the receipt.

Step 1

Press the '**MAIN MENU**' key, select '**BATCH**' from the Report and Terminal menu and then select '**REVIEW**'.



Step 2

The last transaction performed will be displayed. You have the option to scroll through the available transactions using the '**ARROW**' keys. A typical transaction summary is shown to the left.

Error messages

(When inserting, swiping a card or keying in the card number)

When a Chip Card is inserted, swiped or the long card number is typed in, the terminal will check against a number of parameters downloaded from the Castles technology system. If the terminal rejects the card it will display one of the following messages:

ACQUIRER DISABLED	The terminal has become logged off from your acquirers. Please contact the helpdesk to have your terminal logged on again.
CARD ERROR	The magnetic stripe could not be read when the card was swiped. Check that it was swiped the correct way round and try again, or try a different card. If problems persist, please contact the helpdesk.
PLEASE REMOVE CARD	The chip could not be read when the card was inserted. Check that it was inserted the correct way round or try an alternative. If problems persist, please contact the helpdesk.
EXPIRED CARD	The card inserted is past its expiration date or the date on the terminal is incorrect.
INVALID CARD	The check digit (last digit) of the card number entered is incorrect. Double check you have the correct number and try re-typing carefully.
MAN ENT NOT ALLOWED	Typing in the number of this type of card is not allowed by the Card Issuer. You must only insert or swipe it.
SETTLEMENT REQUIRED	If the Settlement procedure is not completed on a regular basis, the terminal's batch record of totals will become full. The Settlement procedure must be performed before you can resume taking transactions. (See page 66 for more information)
STORE FULL	The terminal stores offline authorised transactions until it next successfully connects to your acquirer. To prevent delays in funds reaching your bank account, the terminal will only store a limited number of transactions before displaying this message. Please complete a settlement. (See page 66 for more information.) Please contact the helpdesk immediately if a settlement does not resolve the issue.
UNSUPPORTED CARD	It is not permissible for the card number to be used on the terminal. PLEASE NOTE: This message is usually the result of typing in the card number incorrectly. Check you have the correct number and try re-typing carefully. If problems persist, please contact the helpdesk.

Terminal problems

Terminal screen is blank	**Countertop models (V3C)** Check that the power supply or mains cable is plugged into a working electrical wall socket and that any switch is on. If an extension cable is being used, check the fuse. Check that the power supply is connected to the socket on the base of the terminal. **Portable models (V3M2 Wi-Fi and V3M2 GPRS)** Ensure a battery module is fitted. Hold down the power button located above red 'X' key at the terminal keypad until display illuminates. **If the terminal does not beep and turn on:** Connect the power USB Type B cable into the power source and onto the USB port on the left hand site of the terminal or place on a powered charging stand. Hold down the power button located above red 'X' key on the terminal keypad until display illuminates. PLEASE NOTE: If problems persist, please call the helpdesk.
Battery module not charging (SPg7 Wi-Fi and SPg7 GPRS)	**If the battery module is not charging:** Check the power supply or mains cable is plugged into a working electrical wall socket and that any switch is on. If an extension cable is being used, check the fuse.
	Check that the power supply is plugged into the socket on the rear of the charging stand or the rear of the terminal.

Terminal problems

Wi-Fi access point doesn't turn on (V3M2 Wi-Fi)	**If the Wi-Fi access point power indicator light doesn't turn on when it is plugged into the mains:** Check the power supply or mains cable is plugged into a working electrical wall socket and that any switch is on. If an extension cable is being used, check the fuse. Check that the power supply is plugged into the correct socket on the Wi-Fi access point.
Screen appears frozen, or terminal does not react to inserting a card	**If the screen appears frozen and doesn't react to key presses or inserting a card:** Turn the main terminal off, wait 10 seconds then turn back on again using the power button located at above red 'X' key on the terminal keypad.
Receipts print out blank	**If the paper is feeding through but appears blank:** Your terminal uses thermal paper rolls to print receipts. This paper will only print on one side. When the rolls supplied with the terminal are used up, you must obtain replacements from the supplier recommended by your leasing company. Check your paper rolls Check that the roll is loaded the correct way round. See the Quick Reference Guide or the paper loading section within this User Manual for more information. Only use paper from an authorised supplier for Castles terminals.

Please note: If the above suggestions do not resolve the problem, please contact the helpdesk.

Communication problems

V3C(dial only)

The normal sequence of messages displayed during a transaction using a dial connection is:

CONNECTING VIA DIAL,
CONNECTION MADE, PROCESSING NOW,
APPROVAL XXXXXX

CONNECTION MADE, PROCESSING NOW

This message indicates the terminal has connected successfully. In this case, the following display will be a response from the acquirer.

(See Appendix A for common transaction responses.)

If the terminal fails to connect on the first try, it will make two further attempts to connect before void-ing the transaction. The screen will display:

CONNECTING VIA DIAL, ATTEMPT 2
CONNECTING VIA DIAL, ATTEMPT 3

One of the following error messages may also be displayed:

LINE IDLE

The terminal has detected the presence of a line and attempted to dial but is experiencing a problem connecting.

- The line may require a prefix number to dial out on, for example a **9.**
- The number the terminal dials may not be working on your phone line.
- The terminal may be connected to a broadband line without a DSL filter.
- A third party call service may be in use on the line.

LINE BUSY, WAIT

The terminal is not detecting a normal dial tone on the telephone line.

- The line may be in use, dead or faulty.
- A telephone cable or adaptor may be faulty.
- The terminal may not be connected or the connection to the line is loose.

Please note: Please ensure you are using the telephone cable supplied with the terminal. Other telephone cables may not be compatible.

Communication problems

V3C (IP with dial backup)

The normal sequence of messages displayed during a transaction using an IP/Ethernet connection is:

CONNECTING VIA IP,
CONNECTION MADE, PROCESSING NOW,
APPROVAL XXXXXX

CONNECTION MADE, PROCESSING NOW

This message indicates the terminal has connected successfully. In this case, the following display will be a response from your acquirer.

(See Appendix A for common transaction responses.)

If the terminal fails to connect on the first try, it will make a two further attempts to connect before reverting to dial backup. The screen will display:

CONNECTING VIA IP, ATTEMPT 2
CONNECTING VIA IP, ATTEMPT 3

One of the following error messages may also be displayed:

LINE IDLE

The terminal cannot make a connection.

The Ethernet cable may not be connected.

- Your router or LAN (Local Area Network) may not be working properly.
- Your ISP (Internet Service Provider) may be experiencing problems.

CONNECTING VIA DIAL

The terminal has failed to connect 3 times using IP and has reverted to dial backup. The terminal will try a maximum of 3 times to connect via dial and then void the transaction if it cannot connect.

If this happens, please call the helpdesk as soon as possible to ensure your terminal operates at its optimum speed.

Communication problems

V3M2 GPRS

The normal sequence of messages displayed during a transaction using a GPRS connection is:

CONNECTING VIA IP,
CONNECTION MADE, PROCESSING NOW,
APPROVAL XXXXXX

CONNECTION MADE, PROCESSING NOW

This message indicates the terminal has connected successfully. In this case, the display will show the response from your acquirer.

(See Appendix A for common transaction responses.)

If the terminal fails to connect on the first try, it will make a two further attempts to connect before voiding the transaction. The screen will display:

CONNECTING VIA IP, ATTEMPT 2
CONNECTING VIA IP, ATTEMPT 3

One of the following error messages may also be displayed:

LINE IDLE

The terminal cannot make a connection.

- There may be low/no GPRS signal
- There may be no SIM card installed

see page 28 (Icons index) for details

Please note: GPRS terminals come with a SIM card pre-installed by Castles Technology. If there is no SIM card installed, a warning will display at power up. If this happens, please call the helpdesk.

DO NOT remove the SIM unless instructed by the helpdesk.

DO NOT install your own SIM.

Communication problems

V3M2 Wi-Fi

The normal sequence of messages displayed during a transaction using a Wi-Fi connection is:

CONNECTING VIA IP,
CONNECTION MADE, PROCESSING NOW,
APPROVAL XXXXXX

CONNECTION MADE, PROCESSING NOW

This message indicates that the terminal has connected successfully. In this case, the following response displayed will be from your acquirer.

(See Appendix A for common transaction responses.)

If the terminal fails to connect on the first try, it will make a further two attempts to connect before voiding the transaction. The screen will display:

CONNECTING VIA IP, ATTEMPT 2
CONNECTING VIA IP, ATTEMPT 3

If the terminal fails to connect, check the following (in this order):

- The terminal may be out of the Wi-Fi range of the Wi-Fi access point. If possible, move the terminal closer to the Wi-Fi access point.
- Check the Wi-Fi access point is turned on & plugged in.
- Ensure the Wi-Fi access point is correctly connected to your Internet access point.
- The terminal may not be properly configured to the Wi-Fi access point.

Appendix A
Transaction and terminal responses

APPROVAL or AUTHORISED	The word 'APPROVAL' or 'AUTHORISED' plus a 2 to 6 digit Approval Code indicates the transaction was approved by the Card Issuer.
CARD BLOCKED	The Card Issuer has blocked the card from use.
CALL AUTH CENTRE	A call to the Authorisation Centre is required to complete the transaction.
COMMS FAIL	The terminal is unable to contact the acquirer.
DECLINED	The transaction has been declined by your acquirer or the Card Issuer.
DECLINED BY CARD	The chip on the card decided to decline the transaction.
HOST DECLINED	The terminal has received a decline response from the acquirer.
INVALID TRANSACTION	The attempted type of transaction is not allowed on the terminal.
DECLINED, KEEP CARD or PICK UP CARD	The merchant must attempt to retain the card by reasonable and peaceful means

Appendix B
CVV2 and AVS responses

DATA MATCHED	The address, postcode and CVV2 code data supplied have all matched the data held by the Card Issuer.
DATA NOT MATCHED	The CVV2 code and one (or both) of the address details has not matched the data held by the Card Issuer.
DATA NOT CHECKED	Your acquirer has not checked the address data that has been typed in.
SEC. CODE MATCH ONLY	The CVV2 code typed in has matched the data held by the Card Issuer but one (or both) of the address details did not.
AVS MATCH ONLY	The address details typed in have matched the data held by the Card Issuer but the CVV2 code did not.

Appendix C
Terminal functions from the menu system

The following terminal functions can be initiated from the Menu System.

Reprint	Allows the user to reprint a receipt of the last transaction in the current batch. Ensure the terminal is displaying the Welcome screen. Press the '**F1**' key once to display the Reports and Terminal Menu. Select '**REPORTS**'. Select '**REPRINT**'. If prompted, press the '1' key to print the last receipt or press '2' followed by the invoice number for the receipt you would like reprinted.
Printer Test	Allows the user to test the printer. Ensure the terminal is displaying the Welcome screen. Press the '**F1**' key once to display the Reports and Terminal Menu. Press the down '**ARROW**'. Select '**TESTS**'. Select '**PRINTER**'. Select '**RECEIPT**'. A test receipt will be printed.
Paper Feed	Ensure the terminal is displaying the Welcome screen. Press the '**F1**' key once to display the Reports and Terminal Menu. Press the down '**ARROW**'. Select '**SETUP**'. Select '**PRINTER**'. Select '**PAPER FEED**'. Select '**PAPER FEED**' which feeds the paper 5mm on every key press.

Appendix D
Terminal functions using 'Functions' shortcut

The following functions can be initiated by pressing the 'Functions' key on the Transactions Menu and entering a two digit number (see table below). You may be asked to enter a password before the function can be activated. This facility is often quicker than using the 'MENU' system. Please only use those functions listed below.

Function	Number
Change date and time	10
Paper feed	15
Power saving	44
Reprint last transaction	72
Printer test	82
Change local password	90
Local options (passwords)	97

Appendix E
Set a PABX digit(s)

Terminals with a dial connection come pre-configured with the option to dial a 9 prefix digit before dialling out. By default.

If you require a PABX Digit, please call the helpdesk.

Portable terminal Vega 3000
Charging Stand (Top)

Charging points
These points will convey the power from the base to the Vega 3000 to charge the battery

Power Light
Light will show as green when the power supply is connected and turned on.

Charging Stand
(Product may vary)

For more information regarding these accessories and how to obtain them, please contact your terminal leasing company. Additional accessories (such as mounting poles) may also be available from third party suppliers.

Portable terminal Vega 3000
Charging Stand (Back)

Cable tidy clip
Used to keep cables tidy, secured and protected.

Rubber feet
To prevent sliding of the unit on slick surfaces

DC 9V input power supply

Appendix F
Privacy shield

The PCI Security Standards Council specifies International Standard ISO9564 for protection against fraudulent observation of the PIN during PIN entry.

You must have a privacy shield fitted to your PIN entry device unless one of the statements below is true:

- You only perform keyed transactions, e.g. in a mail-order business without the cardholder present.
- Cardholders can enter his/her PIN while holding the terminal in his/her hand.

Terminal operation

AVS – Address Verification System
A security method used for Customer Not Present keyed transactions to help reduce fraud. This method confirms the house number and numbers from the postcode of the cardholder's registered address. (Not applicable on international cards.)

Batch
The store of transaction totals in the terminal.

CVV2
Card Security Code (also known as CVV, CV2, CVC, CVVC and CSC). This is usually used for keyed transactions to reduce fraud. The CVV2 code is a 3 digit number found on the signature stripe, or for American Express, a four digit code on the front of the card.

Cashback or PWCB
A value-add service which allows you to debit a cardholder's debit card and hand over the equivalent value in cash.

MID – Merchant Identification
A 7-16 digit number assigned by your bank to identify a merchant. Often abbreviated to MID. Additional card schemes may have separate MIDs.

PIN – Personal Identification Number
This is usually a 4-digit number entered at the point of sale to validate the cardholder.

End-of-day banking/settlement
The procedure whereby the terminal checks the totals it has stored in its Batch with the totals stored at your acquirer.

Terminal ID (TID)
A unique number assigned to each terminal.

UKCA – UK Cards Association
The organisation defining the rules and standard for the operation of most Point of Sales equipment in the United Kingdom and Ireland. Formerly known as Association for Payment Clearing Services (APACS).

Communications

Wi-Fi access point
A device that allows a Wi-Fi terminal to connect to a host or acquirer. The access point can communicate with an external network either via dial or network communications.

Wi-Fi
A wireless method of short range communication usually found in handheld devices.

Glossary
Communications

Broadband
Internet. Broadband systems are typified by being always connected and having faster connection speeds than dial-up. The most popular kinds of broadband include ADSL (Asymmetric Digital Subscriber Line) and Cable.

Dial backup
The ability of a terminal to revert to the dial mode of communication in the event of an IP/Ethernet connection being unavailable.

DHCP – Dynamic Host Control Protocol
A system where IP Addresses are assigned to networked equipment automatically.

DSL filter
A device that improves the quality of an ADSL (broadband) enabled telephone line by separating data and voice signal frequencies.

Ethernet
A standard used to physically connect devices together. Networking protocols such as IP can be used over Ethernet connected equipment.

GPRS – General Packet Radio Service
This is a method of communicating data via the mobile phone network.

IP – Internet Protocol
A method whereby data is transmitted over networks such as the Internet (may also be expressed as TCP/IP).

IP address
A number represented in the form XXX.XXX.XXX.XXX which identifies a device on the Internet (for example: 193.129.71.130). These numbers are the networking equivalent of telephone numbers.

MAC address – Media Access Control address
An individual address given to every piece, of Ethernet networking equipment. This address is always marked on Spire Payments equipment containing such an address. Do not confuse with Message Authentication Certificate: a certificate used in the UKCA Standard 70 message protocol.

PABX – Private Automatic Branch eXchange.
Usually found as part of a larger telephone system, requiring the user to press a number on their telephone to make an external call.

TCP port
A number representing a service at a particular IP address.

Software license