P2PE EVO TERMINALS IMPLEMENTATION GUIDE

V2.1

verifone.co.uk

Verifone®

REVISION HISTORY

SOFTWARE VERSION

This document refers to the PAYware Ocius VX Evolution software V03.52.00.XX and above.

DOCUMENT REVISIONS

The following table summarises the main changes made to this document:

VERSION	AUTHOR	DATE	COMMENTS
2.1	ND	Sept 2015	- Added information on virtual keyboard - Added new IP address for P2PE test transactions - Updated VX Evolution Platform table - Auto logoff documented - WebCom URLs updated
2.0	ND	Dec 2014	- Rebranded document in line with recent Verifone rebranding - Added 'REQLASTMSG,' as an Additional Integration Command - Updated documentation in line with P2PE requirements. - Audit Trails and Centralised Logging section c removed - Removed Transax SV - Document title changed to meet P2PE requirements
1.2	JS & ND	June 2014	- VAAD information added - Stay offline functionality documented - Added details on M/Chip, HVP and LVP - Information added on American Express contactless not supported - Account Check added - New terminal screens added - Rebranding of solutions: Sentinel to POS Client, PayPage to Payment Page, and ICP to Gateway - Addition of Account Check transaction type - Document name change and inclusion of PCI PA-DSS requirements - Contis & Pennies added - Status messages amended - Wireless Configuration documented - Terminal images section added - Amended PA DSS compliance table - Comms Down added to response table - Post Confirm Reversal added
1.1	JS	Nov 2013	- Rebranding update
1.0	ND	Feb 2013	- First release of document

TABLE OF CONTENTS

INTRODUCTION

The purpose of this document is to provide integrators and merchants guidance on how to install and configure VeriFone's PAYware Ocius VX Evolution terminal solution with Point-to-Point Encryption (P2PE) requirements.

The VX Evolution is a family of payment devices designed to enhance any market, providing future-proof technology, longer-life design, most advanced security, power-packed performance and ultimate reliability.

Full details are included on all available solutions; ensuring PCI Compliance requirements, installation and integration procedures, additional functionalities available and supported value-added services.

Any changes made to the solution will be recorded in release notes and reflected in this document, where deemed necessary. The document will be reviewed periodically to ensure the information is in line with the solution, and annually in accordance with the P2PE Domain 2 requirements.

A latest version of this document will be distributed to the Engineering departments and to Product Management for distribution to the business.

TERMS AND ELEMENTS USED

NAMING CONVENTIONS

The following table describes some of the key terms and acronyms and their definitions which are used within this document:

CONVENTION	DESCRIPTION
Acceptor	The organisation (usually a merchant: e.g. a shop, restaurant or mail order company) that accepts a card in payment.
Acquirer	The bank which recruits service providers to accept payment cards. Acquirers process a merchant's transactions and pass them into the clearing system to allow financial settlement.
Cardholder	A person to whom a payment card has been issued.
Cardholder Verification Method (CVM)	A means of identifying that the person presenting the card is genuine. This may, for example, be performed by use of a PIN or signature in a retail outlet or by PIN at an ATM.
Card Issuer	The bank or building society or company which issues a payment card to the customer.
Cardholder Not Present (CNP)	A transaction where the merchant does not have physical access to the card (e.g. through telephone, mail order or Internet transactions).
Card Schemes	Organisations which manage and control the operation and clearing of transactions. Banks and building societies must be members of the appropriate scheme to issue cards and acquire card transactions. Examples of schemes are Visa, MasterCard, Switch, American Express and Diners Club International.
EMV	The internationally agreed standards for chip payment cards. EMV standards are owned and managed by MasterCard and Visa.
EFT (Electronic Funds Transfer)	EFT is the process of transferring money from one account to another through electronic systems.
Fallback	A transaction that is verified by a method other than the optimum available on both the card and the device. For example, a chip and PIN transaction would fallback to signature or key entry.
Offline	An operating mode in which the electronic terminal does not connect to a central server. The purchase is authorised without checking with the Card Issuer. The transaction is later transferred to the processing system for payment.
Online	An operating mode in which the terminal connects to a central server to check cardholder and account details with the Card Issuer before authorising a payment. The transaction details are transferred automatically to the processing system, either immediately or later.
PIN (Personal Identification Number)	A set of numeric characters, usually a four-digit sequence, used by the cardholder to verify identity at the POS or a customer activated terminal, such as an ATM.
PIN pad	The numeric pad into which a cardholder keys their PIN to authorise a transaction. PIN pads may be fixed or portable. PIN pads are also referred to as PIN Entry Devices (PED).
Payment Gateway	Verifone Managed Service Payment Gateway which is a level 1 PCI DSS certified payment processing infrastructure that delivers fast, secure authorisation and processing of card payments.
POS (Point of sale)	POS is where a transaction is completed.
Managed Service	Verifone provides a customised solution to meet each merchant's needs by processing card payments from various solutions, as well as reducing their PCI compliance issues.
PCI DSS (Payment Card	Security standard to enhance payment card data security. Verifone are fully

Industry Data Security Standard)	accredited with PCI DSS level 1 certification.
VAS (Value-added Services)	VAS are additional services offered along with the solution, such as gift cards, loyalty schemes etc.
WebCom	Verifone's web-based online management and reporting tool.
Integration Key	An integration key is used to allow AES encryption, which consists of a private and public key.
Integration Testing	Pre-testing with merchant's server in order to troubleshoot prior to fully integrating with the solution.

ELEMENT USAGE

The following element usage is used throughout the document:

- **'O' (Optional)** – element does not have to be present.
- **'M' (Mandatory)** – element must be present and populated with a value.
- **'C' (Conditional)** – element is dependent upon the usage of one or more elements and/or their results.

OVERVIEW

VX EVOLUTION PLATFORM

The VX Evolution family offers advanced technology capabilities such as Near Field Communication (NFC), Europay/Mastercard/Visa (EMV), tighter security with PCI PTS 3.0, higher-level performance and provides end-to-end encryption and tokenisation.

This guide is applicable to the following solutions and versions:

SOLUTION	PCI PTS	PA-DSS VERSION	SOFTWARE VERSION	KERNEL VERSION	DATA ENCRYPTION	LAYER 1	LAYER 2	FALLBACK
PAYware Ocius VX 820 IP/DUET	3.X	V3.6	V03.52.01.x	6.2.0	DUKPT	168-bit 3DES	N/A	None
PAYware Ocius VX 820 POS Client PED	3.X	N/A	v03.09.13.x	6.2.0	DUKPT	168-bit 3DES	N/A	None
PAYware Ocius VX 680 Bluetooth	3.X	V3.6	V03.52.01.x	6.2.0	DUKPT	168-bit 3DES	N/A	None
PAYware Ocius VX 680 GPRS	3.X	V3.6	V03.52.01.x	6.2.0	DUKPT	168-bit 3DES	N/A	None
PAYware Ocius VX 680 Wi-Fi	3.X	V3.6	V03.52.01.x	6.2.0	DUKPT	168-bit 3DES	N/A	None

The VX Evolution payment devices are specifically designed for customer present environments; including retail and hospitality, with a wide choice of customer-facing payment devices to suit the specific needs of each merchant with multiple connectivity options and features.

POINT-TO-POINT ENCRYPTION (P2PE)

Point-to-Point Encryption (P2PE) strengthens the security of VeriFone's existing PAYware Ocius POS Client solution using the SRED module, providing encryption of PCI-branded payment cards from the point of card data capture. SRED is the only PCI-approved encryption method used in this solution, which cannot be replaced with any other types of encryptions.

PCI-branded payment cards are used for EFT (Electronic Funds Transfer) payments, which act in accordance with the PCI standards, for example debit or credit cards. Non-PCI-branded payment cards refer to the Value-added Service cards or any other non-PCI compliant payment cards.

As part of P2PE when a payment card is presented, the PAN (Primary Account Number) is encrypted within the terminal using the SRED (Secure Reading and Exchange of Data) module. The SRED module will use ADE (Account Data Encryption) SRED firmware to encrypt PAN information using 3-DES (Triple Data Encryption Standard) algorithm, prior to being passed to the terminal P2PE application. The terminal application is used to process the transaction and will not bypass Key Management and key-loading functions or store any Cardholder Data (CHD). Once the encrypted data is passed onto the terminal application, the application code securely deletes any PAN information from the terminal.

In accordance with the P2PE requirements, the terminal application will only export PAN/card data that has been encrypted by the firmware of PCI-approved POI device and will not export any clear-text data outside of the terminal. The decision whether to output the CHD as encrypted or in clear-text is based upon the ADE SRED "Whitelist" file only.

Please note: *This document has been produced in accordance with the related P2PE Domain 2 requirements for this solution.*

SRED

The VX Evo terminals are P2PE compliant devices which do not support any other form of encryption and only the SRED module will be utilised.

When SRED is activated, the terminal application will call ADE SRED firmware function to Derived Unique Key Per Transaction (DUKPT) to encrypt a block of memory which contains PAN/card data. The SRED firmware will encrypt the data and return to the application three elements that can be used by the Managed Service to decrypt and therefore read the original data in the clear:

1. Encrypted data (Triple-DES encrypted)
2. A Key Serial Number (KSN)
3. Initialisation Vector (IV)

As PAN/card data remains fully encrypted throughout this process, and the merchant has no ability to decrypt the data, the information is effectively removed from the merchant's system.

Please note: *SRED is automatically enabled on the PED when a P2PE compliant software is loaded, and cannot be disabled once activated.*

Card data obfuscation will be performed by the SRED module and cannot be overridden by the application. The application can only select the obfuscation level required, either first 6 and last 4, or last 4 to be returned in clear-text.

In the event that the SRED module fails and DUKPT encryption is not available, the terminal application will inform the POS of this failure and disable the ability to start EFT transactions. In addition, the terminal will display “EFT Transactions Not Allowed” and prompt to contact VeriFone support team (Merchant Helpdesk/Technical Services).

Whitelist

The Whitelist file resides on the terminals and contains range definitions for only the Non-PCI-Branded payment cards (Non-EFT cards). All card ranges that are required to be returned in clear-text will need to be added to this file. All PCI-Branded ranges (EFT cards) will remain in the IIN (Issuer Identification Number) table resulting in the card details being encrypted and masked.

Please note: *The Whitelist file limits the output of clear-text data to only the Non-PCI-Branded payment cards.*

Depending on the card ranges in the Whitelist file, the PAN of a Non-EFT card may appear as clear-text or obfuscated. The only way to output clear-text data for Non-EFT cards is to include the card range within the Whitelist file. The CARDWAIT function is used via integration messages to retrieve card data in either clear-text or obfuscated/encrypted format, dependent upon the card range presence in the Whitelist file.

Please note: *In accordance with certification requirements, the PAN of an EFT card will always output as obfuscated on receipt printing (starred PAN with only showing the last 4 digits).*

When a card is presented, the terminal application will perform a Whitelist lookup on PAN and determine one of the following:

- If the lookup succeeds then the card will be considered as a Non-PCI-Branded card and the CHD information will be returned as clear-text and processing will continue as normal. However, if the matched record has been configured to use masked PAN then only the first 6 digits of the PAN (and/also the last 4 digits, depending on the masking scheme used) will be output.

- If the Whitelist lookup fails then the card will be considered as PCI-branded card and the card data returned will be encrypted and masked.

The Whitelist file has been designed to use “From and To” key-pairs, whereby it involves identifying only one range definition within the Whitelist that matches the PAN.

When the Whitelist file is initially loaded onto the terminal, it will be unencrypted. The file will be accompanied by a valid VeriShield file-signing signature file, which is a file with a matching filename containing a P7S extension that has been generated by authorised personal using VeriShield file-signing tool. Once the Whitelist file has been authenticated by OS via the signature file, it is stored in normal flash memory alongside the signature file (signed with a SHA-256 certificate). The application code will authenticate the file against the signature file at every start--up and if it fails authentication, then the application will disable Whitelist lookup. From this point

onwards, everything will be returned encrypted, regardless of whether a PCI-branded/Non-PCI-branded card is presented.

The Whitelist function will use strong cryptography authenticated by PCI-approved ADE SRED firmware on the terminal. Any updates or modifications to the Whitelist file can only be implemented by authorised individuals, using strict Dual-Control Signing procedure.

Please note: *If the Whitelist file is not present on the terminal, then all transactions will be encrypted, resulting in the Non-PCI-Branded cards to fail, if they require data in the clear-text.*

In the event, when a non-conforming Whitelist file is used, the terminal will display the following error "ERROR: Whitelist Failed! Value Adds Disabled" and all transactions will be encrypted hereafter.

Offline Processing/Storage

Transactions stored offline on the terminal will not contain full PAN/SAD information, which includes card-validation codes/values, full-track data from either the magnetic strip or the chip, PINs and PIN Blocks. As such, all non-essential CHD, is removed from the offline record. When a terminal goes into offline mode, it will complete the transaction and create a submission file without the SAD information. This is achieved by a code on the terminal application which automatically removes the SAD information from the file by setting the SAD objects as nothing, leaving only the following CHD on the file:

- PAN (Encrypted)
- Cardholder Name
- Service Code
- Expiration Date

Upon submission, the offline payment information will be retrieved and the encrypted data will be deleted from the terminal. The application will proceed with the submission to the Payment Gateway. If successful, the application will dispose of the transaction object. If unsuccessful, the application will restore the data to the terminal and dispose of the transaction object.

Key Management

Key Management is required to provide new keys to terminals in the event that they expire or are compromised.

The SRED module will be using the DUKPT Key Management scheme, in which for every transaction a unique one-time transaction key (derived from the Initial Data Encryption Key (IDEK)) is generated and then discarded. The IDEK is derived from Base Derivation Key (BDK). BDK is a fixed key generated within VeriFone's PCI-approved secure servers.

The IDEK key can be injected directly into the terminal via the VeriShield Remote Key (VRK) service. The VRK service remotely and securely manages key injection using asymmetric encryption in compliance with PCI to strengthen security. All encryption keys used for DUKPT will be supplied by the VRK service.

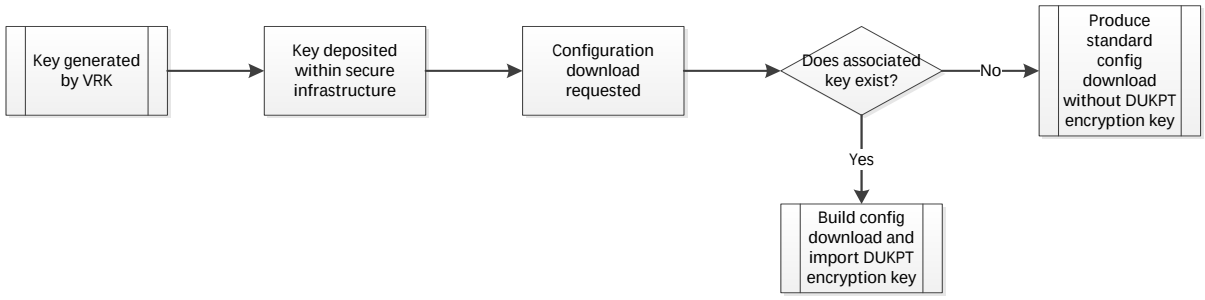
DUKPT will use only the terminal's serial number, prior to being sent to the Point of Sale (POS) for onward transmission to VeriFone's Managed Service. A new DUKPT key is derived for each transaction; therefore, the same key cannot be used more than once. If an individual key is compromised, it does not compromise past or future transactions. PAN/card data is only decrypted once safely inside the certified and secure environment of VeriFone's Managed Service, prior to transmission to the acquiring bank.

As part of the Key Management procedure, only a finite number of encryption keys can be derived from an IDEK. Each key is rotated and a new key is generated via configuration download. When the database produces a configuration download, a check will be performed to look for a key belonging to the Terminal ID (TID) associated with the download being performed. Once an encryption key has been downloaded to the client application, and the download has been confirmed as completed, the stored key will be deleted. The key cannot be reloaded at another date as this would result in the same keys potentially being re-used. No other changes will be made to the download process with the exception of the inclusion of the Whitelist file.

Please note: *Software installations and updates cannot be performed without the use of the PCI-approved Key Management and Dual-Control Signing procedures.*

For detailed instructions on how to use the approved security protocol, please refer to the Software Development Process Requirements document.

The below flow illustrates the Key Management process:



The keys are safeguarded and managed in a Hardware Security Module (HSM), which provide crypto-processing without disclosing any key data. HSMs provide both logical and physical protection of unencrypted BDK keys from non-authorised use.

Server Authentication

The terminal login IDs provided are authenticated against the user's merchant system when it is securely transmitted to the Verifone server using hash PIN with SHA-512.

Please refer to the PIM document for instructions on how to securely configure the terminal application.

Change Control

All changes to the solution will be implemented in accordance with the change-control procedures within VeriFone.

Any software upgrades or configuration downloads will be completed remotely by authorised personnel using PCI-approved Dual-Control Signing and Key Management procedures. For more details, please refer to the Remote Software Upgrade/Configuration Downloads section within this guide.

All releases of the P2PE VX Evolution terminal solution will be provided with release notes, detailing any impact of the changes and subsequently updated within this guide if necessary. Release notes are available via WebCom or by contacting the Technical Services team.

Vulnerability Assessment

As part of the quality assurance testing, authorised personnel will perform vulnerability testing on all the Evo terminals in order to detect any discrepancies such as buffer over-flow, prior to releasing the software.

Dual-Control Signing

In accordance with PCI regulations, VeriFone will ensure all installations and updates to the solution are achieved using approved Dual-Control Signing procedure, by authorised personnel only, preventing unauthorised changes to the application software.

Cryptographic signing cards will be used to authenticate the application software to ensure the software has not been tampered with or corrupted in any way throughout the development life cycle.

The Dual-Control Signing procedure will consist of the following for each software build produced:

- A signing kit
- Two authorised terminal developers
- An Engineering Manager with access to the signing kit

A signing kit consists of a signing reader and a signing card, which is used to authenticate the code. Use of the signing card will not be permitted with only one password; authentication passwords from both authorised developers will be required. Once authentication is approved, developers will be able to update the application software, ensuring Dual-Control signing procedure is used at all times for any updates.

All signing kits will be stored in a PCI-approved protected environment, which is accessible to authorised personnel only. All source and usage details of each Dual-Control Sign will be recorded and stored securely.

Please note: *Merchants are restricted from installing terminal software applications, only software upgrade will be accessible via WebCom. The terminal application installation is controlled by authorised personnel with Dual-Control Signing privileges.*

All software updates will be performed via remote downloads, using the Key Management procedure to prevent unauthorised updates.

For security reasons, full instructions of the Dual-Control Signing procedure are not incorporated within this guide. For more details, please refer to the Software Development Process Requirements document.

PIN PADS

Verifone's PIN pads open opportunities for credit, debit and other types of payment that require customers to enter a personal identification number (PIN).

VX 820

The VX 820 PIN pad is an advanced version of Verifone's V^X 810; enhanced with colour display, touch-screen and contactless capabilities. Its advanced and intuitive technology provides reliable and robust customer-facing PIN pad which is easy to use in retail and hospitality environments.

The PIN pad provides merchants with a single-port connectivity offering the capability to install the terminal via USB, Serial or Ethernet connections using the appropriate cable.

The VX 820 PIN pad can be used on its own with an IP (Internet Protocol) connection. It is fully programmable; securely and efficiently handles all payment needs including magnetic card, EMV and contactless transactions.

When using the VX 820 as a PIN entry device (PED), it can be connected to the local area network and configured to return voucher information via integration, allowing the merchant to produce receipts at the Point Of Sale (POS) including all transactional information. Receipts are produced using the Voucher Record details. The solution is an integration only (via either RS232 or socket connection) payment terminal, with all on-screen menus disabled.

COUNTERTOP SOLUTIONS

Countertop solutions provide great customer service through efficiency at checkout. Solutions are specifically designed for high volume, high traffic and retail environments. Countertop solutions provide the value-added benefits including loyalty programs, mobile phone top-up, e-gift cards and (DCC) dynamic currency conversion.

VX 820 DUET

The VX 820 Duet known as the “All In One, Times Two” for its merchant-facing countertop base with a customer-friendly handover PIN pad is a dual layer design benefiting both merchants and customers with its ease of use technology.

The countertop device provides all the features and functionality of the VX 820 PIN pad with a sturdy cradle (base station) for merchant use. The base is built with a printer neatly tucked in the base and the peripheral and communication ports located on the back.

PORTABLE

Verifone’s portable (wireless) solutions deliver the extended coverage and flexibility that merchants need to accept payment anytime, anywhere. The portable payment devices provide GPRS, WiFi and Bluetooth connectivity for optimal usability in hospitality environments. This means there are no call charges and enables the terminal to be used in virtually any location, with transactions completed in a matter of seconds.

VX 680

Verifone’s VX 680 payment device is one of the world’s smallest, fully functional portable devices designed for robust performance. VX 680 devices are specially built with durable components to withstand even the harshest environments.

The VX 680 is tailored specifically to the needs of merchants on the move, from delivery services and stadium vendors to restaurant pay-at-table applications. The device’s 400 MHz ARM 11 processor provides merchants with 3 x faster transaction processing time encouraging more sales.

CONTACTLESS PAYMENTS

In order to process contactless transactions with POS Client, a contactless-enabled device is required. The VX 820 PIN pad supports contactless transactions through an integrated contactless module for EFT transactions.

Please note: *The contactless functionality is optional and only available if configured at merchant account level. For more details, please speak to your Verifone Sales Account Manager.*

The following transaction types are supported for contactless transactions:

- Purchase
- Refund
- Reversal
- Account Verification

Other transaction types such as cash advance, PWCB, CNP and value-added services are not currently supported.

The contactless devices use near field communication (NFC) to process payments by holding the card against the contactless-enabled reader. The feature offers an on-screen tap zone displaying the contactless logo (as illustrated below) on the PED for optimised user experience:

The contactless transaction limit provides merchants with the ability to process low-value payments (LVP) of up to £20*, or high-value payments (HVP) over £20; through the use of PayPass (service developed by MasterCard) M/Chip, magnetic swipe readers and contactless-enabled devices such as mobile devices, smart card readers and key fobs.

Please note: *In order to support contactless HVP, terminals must be accredited to Visa's Contactless Payment Spec 2.1.1 and MasterCard's PayPass Reader Spec 3.0.*

** The value of £20 is subject to change in accordance with scheme rules.*

The service supports processing of the following contactless transaction methods:

- M/Chip – EMV (Europay MasterCard Visa) based application
- Magnetic stripe swipe – Track 2 equivalent data method
- Chip and PIN

Low-Value Payments (LVP)

Provided the total transaction amount is less than the value of £20, a low-value contactless payment can be processed. If the amount is over £20 in value, then the sale can be processed as a standard chip and PIN transaction or a high-value payment transaction, only if the merchant account is enabled to accept HVP.

Processing an LVP transaction imposes a low security risk, as the transaction limit is set to £20 and after certain amount of transactions; the cardholder is prompted to enter their PIN.

High-Value Payments (HVP)

High-value payments allow merchants to process higher values over £20, through supported PayPass contactless enabled devices and if enabled on the merchant system.

HVP contactless transactions must be performed with Cardholder Verification Method (CVM). CVM will not be used to process transactions below the LVP limit of £20; this is known as NO CVM. If there is no Cardholder Verification Method Result (CVMR) floor limit present on the PED when a HVP transaction is processed, then the transaction will fall forward to a contact transaction (if supported), or declined. A contact transaction prompts the cardholder to insert the payment card into the PED.

> ***Please note:*** *If no contact interface is available, i.e. both the PED and the contactless device is contactless only then the transaction will be declined.*

The PED is able to apply different limits based upon other parameters used such as the Application Identifier (AID) read from the payment card. This allows the handling of the subset of contactless devices which are different from the general contactless CVM limits, e.g. co-branded cards may have a higher CVM require limit when used in the co-branded stores.

> ***Please note:*** *CVM processing is driven by the value of the transaction, the contactless device used and the configuration on the PED.*

To process HVP transactions, merchants must have an agreement with their acquirer and ensure HVP is enabled at the account level within their merchant system. For more details, please contact your Sales Account Manager.

> ***Please note:*** *Currently, the only acquirer which supports HVP contactless refund transactions is Barclays. When a refund is processed, the cardholder will be asked to provide a signature.*

M/Chip

M/Chip is EMV-compliant application providing both debit and credit functionality in one integrated solution, on a smart card chip. With M/Chip, merchants can support interoperability between smart cards such as MasterCard, Maestro and Cirrus-branded and chip-enabled terminals.

Please note: *American Express ExpressPay is not supported for contactless transactions. Attempts to process any American Express contactless transactions will be declined.*

The use of M/Chip will enable faster transaction processing and ensure reliability and security of the transaction.

For more details on this service, please refer to MasterCard's M/Chip Implementation Guide provided by the issuer.

Magnetic Stripe Swipe

Signature verification is not applicable to all form factors, i.e. mobile phones; however, some may require signature verification with contactless transactions.

If an HVP transaction is being carried out using a swipe card, the cardholder will be asked to provide a signature. Similarly, a cardholder using an ICC card will be asked to enter their PIN.

Please note: *Signature verification will not be required for a LVP transaction.*

Consumer/On Device Cardholder Verification Method (CDCVM/ODCVM)

Consumer devices that contain a payment card application can be used in a contactless-enabled environment, i.e. cards, fobs, phones etc.

If a HVP transaction is processed via a mobile device, cardholders will be prompted to enter an Online PIN or On Device Cardholder Verification Method (ODCVM) using a CDCVM code.

The CDCVM code entered by the cardholder is verified against the CDCVM stored within the terminal.

Please note: *The CDCVM code is not the same as card PIN or terminal PIN. Only supported mobile phones can use this functionality.*

The CDCVM code will either be entered on the terminal before the transaction, allowing the CVM details to be presented during the initial tap of the contactless device. If the transaction exceeds the contactless CVMR limit then the cardholder will be prompted to enter the CDCVM code on their device and re-present it to the terminal for second tap and transmission of the CVM details. For example: if CVMR is set to £15.01, the CTLS floor limit is set to £20.00 and the transaction value is £20.00, then upon presenting the card for payment, the terminal will prompt "Please see phone" on the terminal.

Online PIN

The use of Online PIN verification for HVP contactless transactions will only be applicable to European countries that support Online PIN verification.

TOUCH SCREEN & KEYPAD

Terminals on the Evolution platform offer a graphical user interface with touch-screen capabilities, integration PIN pad and full range of processing capabilities.

The colour display screens provide options in the form of icons to facilitate operation; such as a **red** 'cross' to cancel or reject an operation, and a **green** 'arrow' to accept or continue onto the next stage:

Additionally, the **red** 'Cancel' icon on the screen and also found on the keypad can be used to navigate back to the previous screen.

Navigation can be performed via touching the options on the screen display, alternatively using the keypad numbers to match the menu option or enter a sub menu, i.e. to select '1. New Txn', press the number key '1' on the keypad.

The terminal keypad is integrated with numeric, alphabets and special characters. To enter an alphabet, use the relevant number key by pressing it recurrently to scroll through the available characters, until the required alphabet is displayed, e.g. for the letter 'V'; press the '8' number key four times on the keypad. Follow the same process to enter a special character.

Please refer to the below table for more details on which number key corresponds with an alphabet or symbol:

KEY	INTEGRATED ALPHABET/SYMBOLS
1	Q Z .
2	A B C
3	D E F
4	G H I
5	J K L
6	M N O
7	P R S
8	T U V
9	W X Y
0	, ‘ “
*	- +
#	£ ! : ; @ = & /

Alternatively, the alphabets can be entered by selecting the ‘123’ or ‘ABC’ touch-screen option, if available on the screen, this option allows the ability to switch between numeric and alphabet characters. An integrated ‘Alpha key’ (‘ABC’ or ‘abc’) will also be available in certain occasions, to switch between uppercase and lowercase alphabet letters.

To clear an entry, please press the yellow ‘Clear’ key.

Please note: *Menu items will be displayed in a paged format, rather than as a scroll menu.*

In paged format, menu items will always be listed as 1-5, even if there are more options available, which subsequently will be displayed as 1-5 on the following screen. An arrow will be displayed at the bottom of the screen (È or Ç), indicating that there are further set of options available on the next/previous screen. Use the arrow symbols to navigate to the relevant screen, as illustrated below:

Virtual Keyboard

The virtual keyboard is an auto-generated onscreen QWERTY keyboard, displayed only with particular screen prompts that are applicable to the type of input required. For example, the virtual keyboard is displayed when the user is prompted to enter a reference number, conversely if a PIN entry is prompted then the virtual keyboard will NOT be displayed.

The touchscreen capability allows key entry by touching the characters on the screen. In addition, users are able to use the keypad for numerical entries.

The feature is only supported on the VX 820 Duet and IP solutions, and only for the VAAD (Visa Additional Authorisation Data) prompts on the VX 680 terminal.

The following three character modes are available:

- Uppercase alpha characters
- Lowercase alpha characters
- Numeric and symbols

The user is able to switch between the different modes using the ‘ABC’, ‘abc’ or ‘Sym’ key found on the bottom-left of the virtual keyboard, as illustrated below:

Uppercase

Lowercase

Numeric & Symbols

Please note: *If the numeric option is disabled, then the numeric keys will not be displayed on the screen, only the symbols will be displayed. However, the numeric keys on the keypad can be used instead.*

TERMINAL IMAGES

The VX Evolution terminals can be configured to display a single or multiple images as a screensaver while in the idle mode. This can be used by merchants and other customers to display brand logos, special offers, promotions and advertising.

These images can only be downloaded to terminals via software download in WebCom. Screensaver images can be placed in groups of up to 20 images, which will appear on the terminal screen after a configured amount of time (between 5 and 60 seconds). The images will rotate sequentially after a given period of time as defined by the user.

This image screensaver is supported by the VX Evolution range of terminals including: the VX 820, VX 680 Wi-Fi and VX 680 GPRS. See table below for list of supported terminal solutions:

TERMINAL SOLUTION	IMAGE SUPPORT	IMAGE FORMAT	OPTIMUM IMAGE SIZE	MAX IMAGE SIZE
PAYware Ocius VX 680	Multiple	JPG	30kb	225kb
PAYware Ocius VX 820	Multiple	JPG	30kb	225kb
PAYware Ocius VX 820 POS Client PED	Multiple	JPG	30kb	225kb

For full details, see the Terminal Images section of the WebCom manual.

QUICK REFERENCE GUIDES

The following Quick Reference Guides (QRGs) are currently available for the PAYware Ocius VX Evolution solutions:

- VX 820 IP
- VX 820 DUET
- VX 680 Bluetooth
- VX 680 WiFi
- VX 680 GPRS

Quick reference guides are designed to provide users with the basic usage of the solution on how to use the terminal keys, use of terminal options available, how to process a transaction etc., with screen flows.

To obtain a copy of these please contact a Sales Account Manager or the Technical Services Team.

OFFLINE FUNCTIONALITY AND FLOOR LIMITS

If PAYware Ocius is unable to connect to the server then the transaction process will be different from that which the merchant is accustomed to.

To avoid a situation whereby the merchant is left without any payment processing capabilities, PAYware Ocius supports the ability to process transactions in an offline environment. When enabled, which is the case by default, Offline Mode allows transactions to be completed and securely stored on the terminal for submission to the server when the connection is restored. An authorisation code will not be available from the server and as a result, each transaction will prompt for a voice referral if permitted by the chip on the card. In this instance, the merchant will be required to phone their acquirer to obtain authorisation and, if accepted, the transaction will be allocated an authorisation code for the operator to key into the terminal.

The decision to allow the transaction to be processed offline is made by the chip on the card. There will be instances whereby the card does not allow the transaction to be authorised and this will result in the transaction being declined as opposed to voice referred.

As Chip & PIN further evolves, the chips could begin to store a profile of the cardholder's history, including information such as spending patterns and average transaction values. Based upon these profiles, it is believed that card issuers will introduce cardholder specific floor limits. These will allow the chip to base its decision upon the transaction value in relation to the cardholder's floor limit. However, currently this concept has not been introduced and as a result, many offline transactions are rejected outright by the chip. This is not something that PAYware Ocius has any control over as standard; the decision by the chip is final.

There are two options available with PAYware Ocius to add a level of control when faced with this situation, rather than leaving the decision entirely in the hands of the chip. These options are provided by floor limits, which can be configured on the merchant system (it will apply to each and every merchant account within that merchant system), and these are explained in more detail within the next two sections.

Please note: *There are no floor limits configured by default with PAYware Ocius, and any floor limit being added should be carefully considered and discussed with the acquirer.*

EMV Floor Limit

PAYware Ocius has a configurable EMV Floor Limit, whereby all transactions below the configured value inform the card that an attempt to authorise offline is being made (regardless of whether or not there are any issues with the connection). The card may choose to accept, decline or force the transaction online. The EMV floor limit is just one factor taken into consideration as to whether the card can authorise the transaction offline or requires it to be sent online.

In the event that there is a communication issue and the card instructs the terminal to authorise online, in most cases this is expected to result in a Decline or Voice Referral outcome.

This is not a suitable solution to the majority of merchants due to the fact that transactions authorised offline in this manner carry greater risk and therefore higher merchant fees. This is unnecessary in the event that communications are available, which would mean that online

authorisation was available and carry a lower merchant fee due to the cardholder being verified. Most of the current Verifone merchant base has this floor limit set to '0.00' (zero) and it is always Verifone's recommendation that this floor limit is set to zero. The merchant's acquirer is required to approve a floor limit of any value other than zero.

Voice Referral Floor Limit

During normal online operation, the EMV floor limit will remain set to zero when the transaction is initiated. If an EMV floor limit is configured then this will be used alongside the Offline Voice Referral floor limit.

A voice referral is generated whenever there is a communications failure during a transaction, as well as in other instances such as when the card issuer requires further validation before authorising a transaction.

For Keyed and Swiped transaction types only, with many of the PAYware Ocius solutions a Voice Referral response is received from the Verifone Managed Service due to a communications issue, the Voice Referral floor limit configured on the merchant system is applied, if configured.

If the transaction value is above the Offline Voice Referral floor limit, standard voice referral processing will be performed, whereby the merchant is instructed to call the acquirer using the phone number and details displayed on screen by PAYware Ocius.

If the transaction value is less than the Offline Voice Referral floor limit then the transaction will be authorised locally, supplying the authorisation code agreed between the merchant and acquirer and stipulated on the signed agreement between the two parties.

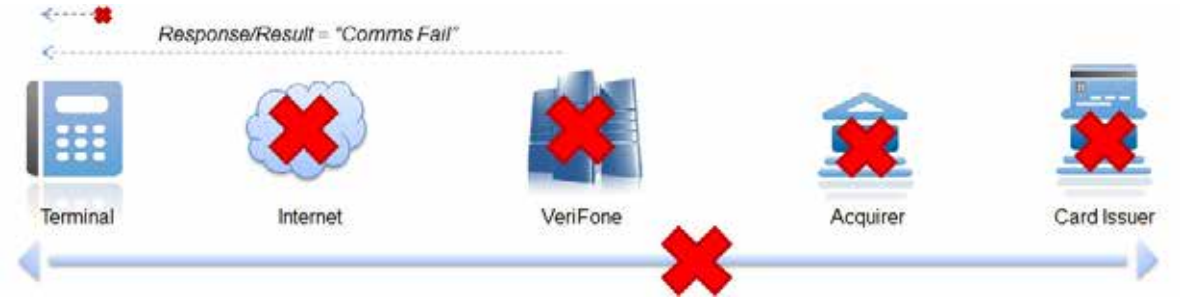
> ***Please note:*** *This floor limit will not be applied in scenarios where the acquirer/card issuer has requested a Voice Referral; instead a Voice Referral screen will be displayed to provide the merchant with the contact and transaction details required to complete the process over the phone.*

Comms Fail Floor Limit

The Comms Fail floor limit is utilised by some PAYware Ocius solutions in the event that after the terminal goes online the Managed Service is not able to obtain an authorisation result from the acquirer or card scheme. In this scenario the Comms Fail floor limit, which ***only allows ICC Transactions*** to have the increased floor limit applied and for offline authorisation to be requested from the card on this basis.

The Comms Fail Floor Limit enables a floor limit to be configured which will only be utilised by the terminal when there are connection issues, which provides an advantage over the EMV floor limit. Should the merchant have an EMV floor limit in place, all cards would be accepted under the floor limit, regardless of if it were possible to attempt to authorise online. Whereas, the Comms Fail Floor Limit provides a mechanism whereby the merchant can ensure that authorisations can be performed online (thus ensuring the lowest interchange rates) unless there are communication issues.

This floor limit will be utilised should the terminal not be able to connect to the Managed Service, in addition to scenarios where the Managed Service cannot connect to the parties further along the processing chain, as shown with the diagram below:



If the PAYware Ocius setup is configured with a Comms Fail Floor Limit, and the transaction value is below the Comms Fail Floor Limit, the terminal will inform the card of the new higher value of the floor limit. The terminal then proceeds with the 2nd Card Action Analysis, informing the card that a communications failure occurred.

It is still possible for transactions to be rejected in this scenario due to the card overriding the authorisation within the 2nd Card Action Analysis stage of the EMV Transaction Flow.

This requires special permission from the acquirer before enabling this feature.

Please note: *Verifone requires a copy of this agreement before the Comms Fail floor limit can be enabled on an account.*

PRE-INSTALLATION

This section is included to draw attention to the requirements, prior to installing the terminal solution with P2PE components.

Please note: *The user must ensure Dual-Control Signing procedure is used to authorise the signature files.*

Only authorised personnel can use Dual-control Signing procedure for signing application binaries and configuration data (e.g. whitelist). This produces signature files against which the original files are authenticated at runtime. Authentication failure renders the terminal unusable. Please refer to the Dual-Control Signing section within this guide, for more details.

MINIMUM REQUIREMENTS

The solution supports the following PCI-approved connectivity methods between the terminal application, POS application and the Gateway service:

- RS232 connection (serial)
- USB connection (serial)
- TCP/IP - outbound Internet access via TCP Ports 29006, 29005 (Gateway) and 29002 (POS)

The TCP/IP connection can be used as a simultaneous communication method, for example in order to communicate between the POS to the terminal and terminal to the Gateway and back to the POS. On the other hand, the RS232 and USB connections can only be used to communicate on a one-to-one basis, i.e. for logging purposes.

Please note: *Connectivity is restricted to the use of the RS232, USB & TCP/IP connections only. Use of any other external communication methods is not permitted with the PAYware Ocius terminal solutions.*

The terminal application is configured using an environment variable which is assigned an IP address of the Gateway, and the port number on it is listening for incoming connections which is port 29000, by default.

Please note: *All P2PE test transactions will need to go through the following IP address: 109.73.122.23.*

For more details on the using the above communication methods, please refer to the Integration Methods section.

Please note: *When utilising the solution with Vista, there may be some User Access Control prompts which either prevent installation or require permission to continue. These will require sufficient network administration rights in order to install the product; ensure that this is in place prior to deployment.*

AVS/CV2 CONFIGURATION

Cardholder Verification Value ('CV2', also known as 'Cardholder Security Code' or 'CSC') checking is now mandated by the card schemes and as a result is enabled on all merchant accounts.

Address Verification System ('AVS') checking is optional and can be supplied as part of the transaction process where applicable, e.g. with mail order cardholder not present transactions.

WINDOWS 98 & WINDOWS NT

Microsoft no longer supports Windows 98 or Windows NT operating systems, therefore Verifone do not recommend their use.

In some configurations, it may be possible to continue to use these operating systems, but it must be stressed that this should only be rolled out for use in a live environment following a satisfactory testing program with the chosen solution. If an unsupported operating system is used, consideration must be given to issues that may arise following any changes to the system that take place after the initial installation.

It should also be pointed out that, once again as these operating systems are no longer supported by Microsoft, that they are not kept up to date with the latest security patches and as such their use may be a breach of PCI-DSS.

To discuss this in more detail, please feel free to speak with your Sales Account Manager or Technical Services Consultant.

PCI DSS COMPLIANCE

As a member of the Payment Card Industry Security Standards Council (PCI SSC), Verifone is dedicated to ensuring merchants and customers alike are protected against card data fraud. All of Verifone's solutions incorporate point-to-point encryption, which can help merchants achieve and maintain PCI DSS compliance.

Transaction authorisation, settlement and management with PAYware Ocius is delivered through a PCI DSS Level 1 certified payment processing infrastructure and is pre-certified with all major UK acquirers.

Verifone's solutions meet all the security requirements of the UK acquirers and major banks and card payment industry. All payment processing is delivered through the Verifone payment gateway.

Verifone's multi-site data centres are ISO27001-certified, and monitored 24/7 and 365 days both on and offsite.

For full information on the Approved PIN Security, please consult the PCI Security Standards website using the following link:

https://www.pcisecuritystandards.org/security_standards/ped/pedapprovallist.html

This section is included to draw attention to the pre-installation requirements from a PCI DSS and PA DSS perspective. For further information regarding installing the solution in-line with these requirements, please see the PA-DSS requirements below[1].

PA-DSS Requirements: *Prior to installing PAYware Ocius ensure the machine is configured to meet PCI DSS requirements, delete any trace files from previous payment applications and ensure that deletion of the data is performed in a secure manner. A deletion tool such as SDelete is recommended which can be downloaded from http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx*

Users are also required to delete any sensitive data gathered as a result of troubleshooting the payment application.

PCI DSS requirements state that the machine must have the latest critical security patches installed as set out within PCI DSS requirement 6.1. As a result, only operating systems which are supported by the vendor can be utilised; therefore, Windows 98, Windows NT4 nor Windows 2000 are supported.

Access controls should be placed around the EPOS system in-line with PCI DSS requirement 7.1 (Appendix F, 3.2), including audit trails (Appendix F, 4.2) showing which users have accessed the machine and assigning a unique ID to each person with computer access (PCI DSS Requirement 8.1).

[1] PA-DSS requirements 1.1.4 and 1.1.5

GATEWAY LIVE & TEST SERVICES

Verifone's Gateway service provides both test and live systems to customers. The test service is available for use during product development, demonstrations, training and any other scenario where the customer may wish to give the illusion of processing real card transactions. The Live service is obviously for use in a live/production environment and will result in money changing hands.

From the point of installation, all Verifone products default to the live settings. If the test service is to be used, please ensure the system is reconfigured accordingly.

Below is a summary of the communication details for each service. These should be passed onto the network administrator to ensure connectivity prior to installation:

SYSTEM	DESCRIPTION	CONNECTION DETAILS
Transaction server	Processes transactions and Is responsible for all account-based terminal updates.	**LIVE** IP Address: 91.207.36.31 RSA Port: 29006 Fallback SSL Port: 29002 IP Address: 91.207.36.33 SSL Port: 29002 Non SSL Port: 29005 **TEST** IP Address: 109.73.122.10 IP Address: 109.73.122.23 (For P2PE transactions) RSA Port: 29006 SSL Port: 29002 Non SSL, some Value-add traffic: 29006
Download Server	Distributes all software-based updates	**LIVE** IP Address: 91.207.36.37 RSA Port: 29006 Fallback SSL Port: 29002 **TEST** IP Address: 109.73.122.14 RSA Port: 29006
WebCom	Online merchant tool	**LIVE** https://reports.paywareocius.com **TEST** https://reports-test.cxmlpg.com

PAYWARE OCIUS RESELLER TRAINING

Whilst the PAYware Ocius installation process has been developed to be as simple as possible, installation engineers are required to attend a PAYware Ocius Reseller Training session with a qualified Verifone engineer.

The course will take attendees through the installation and configuration of a PAYware Ocius solution and answer any questions regarding the process. There is a Reseller Training Overview after the course to check engineers understanding of the core components.

USB TO SERIAL CONVERTERS

USB to Serial converters can provide a useful and largely cost effective way of adding additional support to PC's for serial based devices. Verifone have experienced mixed success with the use of

such devices when attached to PIN pads, and are therefore unable to recommend their use directly. However, some of our customers have sourced adapters that work perfectly well and provide the level of reliability required for such a business critical application.

If the use of a USB to Serial converter is required for your environment, Verifone strongly advise you undertake sufficient testing of your chosen adapter and are entirely happy with its reliability for your requirements. Verifone are unable to accept any responsibility for data communication issues that may arise as the result of using such equipment.

INSTALLATION

The terminals are dispatched preloaded with the latest PCI-approved ADE SRED enabled software, by authorised personnel in VeriFone's secure environment, using Dual-Control signing procedure. Prior to configuring any devices, please refer to the P2PE Instruction Manual (PIM) to ensure configuration is performed in accordance with P2PE requirements.

The terminal software application has been designed as a standalone application, therefore inter-process communication (IPC) is not used by this solution.

Please note: *Due to the nature of the solution, the terminal application does not use any form of internal communication methods to pass clear-text data. The clear-text data is passed to a block of memory within the terminal which is immediately encrypted when SRED is activated, and deleted from the memory.*

AUTO-TIDY PROCESS

When processing a transaction through PAYware Ocius, there are various stages at which PAYware Ocius exchanges information with the Gateway server.

This can be summarised with the below overview:

1. PAYware Ocius exchanges encrypted data with Gateway service which, in turn, sends the transaction for authorisation
2. Gateway service returns authorisation result and authorisation code if applicable
3. PAYware Ocius responds to Gateway service, either confirming or reversing the transaction
4. Gateway service confirms final transaction result and closes connection to PAYware Ocius

Should there be connection issues after PAYware Ocius has sent the transaction to the Gateway service, Gateway is configured to automatically tidy any transactions which have not been confirmed. This will result in the transaction being reversed (declined).

If the connection fails at stage 2 and the terminal does not receive an update from the Gateway service on the authorisation status, then PAYware Ocius will report that it was unable to connect and print 'Void' receipts. The transaction should be reprocessed in this instance.

If the connection fails at stage 3, resulting in PAYware Ocius not being able to send the confirmation message to the Gateway service, it will store the confirmation locally and re-send when the connection is restored. If this 'stored confirmation' is received before the end of day process then the final status of the transaction is updated and sent for settlement on that day. If the stored confirmation is received the next day then the transaction is sent for settlement on that day.

If PAYware Ocius does not receive confirmation of the final transaction result, it will resend confirmation to the server, at which point it will be informed that the transaction has already been completed or that the transaction has been updated as per the confirmation message.

Should there be a problem with the terminal and the software needs to be reloaded then the terminal will need to be returned to Verifone. In this instance, please contact the Merchant Helpdesk who will provide further instructions and process a swap out.

ON-GOING MAINTENANCE & SECURITY

Cardholder Data & Encryption

The PAYware Ocius software application resides on a PIN Pad within a PCI PTS/APACS Common Criteria secure environment providing dual-layer data encryption from the point of card data capture. Sensitive cardholder data is encrypted within the PIN Pad using both 168-bit 3DES encryption (utilising a unique dynamic key system generated using transaction specific data elements) followed by further encryption using a 2048-bit RSA algorithm, before being sent to the Point of Sale for onward transmission to Verifone's Managed Service via a Secure Sockets Layer connection.

Mutual authentication is performed to ensure that PAYware Ocius is interacting with Verifone's Gateway Managed Service. A data segment, using a dynamic encryption key, is attached to each transaction and must be decrypted by the Managed Service, returned to the terminal and is verified by the PED before the transaction is confirmed.

As part of on-going maintenance, and in accordance with PCI PA-DSS requirements, users must ensure that cardholder data is protected and cryptographic keys are managed properly. [2]

PA-DSS Requirements: *All cardholder data must be purged from all locations where it is stored after a customer-defined retention period. Keys used to secure cardholder data against disclosure and misuse must be protected.*

Cryptographic key material or cryptograms stored by previous payment application versions must be rendered irretrievable. Key management processes and procedures for cryptographic keys must be implemented.

Strong cryptography and security protocols must be used for cardholder data transmission over public networks.

Please note: *PAYware Ocius and previous versions of the solution do not store any cardholder data, cryptographic key material or cryptograms on the merchant's system so there is no need for any data purging.*

Sensitive cardholder data is dual layer encrypted prior to onward transmission at the PED. All key management processes are carried out by Verifone's Security & Compliance department.

[2] PCI PA-DSS requirements 2.1, 2.5, 2.6, 2.7 and 11.1.

Further guidance is outlined regarding unique user IDs and access to cardholder data below:[3]

PA-DSS Requirements: *Users are advised to use unique user IDs and secure authentication for administrative access to cardholder data and secure access to PCs, servers and databases with payment applications.*

Cardholder data must only be stored on servers not connected to the Internet.

Sensitive cardholder data must be encrypted if sent over end-user messing technologies and non-console administrative access must also be encrypted.

However, no action needs to be taken by the merchant because PAYware Ocius does not store any cardholder data on the merchant system so there is no access to such data.

Verifone does not support remote access to the solution; however, encrypted log files created on the merchant system may be requested by Verifone engineers. These can be found at <Install Directory>/Logs.

Remote Software Upgrade/Configuration Downloads

Remote downloads provide the ability to update software versions to the latest released versions and download any configuration changes to the terminals. As part of the software upgrade process, the latest PAYware Ocius software update is downloaded onto the application followed by a configuration download onto the terminal. A configuration download will upgrade the terminal software version and all configurations.

PA-DSS Requirements: *There must be a secure delivery of remote payment application updates supported by remote access software.*

Whitelist file updates are provided as part of the software downloads. The OS (Operating System) will authenticate the Whitelist file on all new software versions downloaded onto the terminal.

Due to the nature of the solution, the terminal application software cannot be withdrawn or uninstalled, only upgraded. If you require assistance with this process, then please contact VeriFone Merchant Helpdesk.

Please note: *Any software updates or configuration updates must be performed using Dual-Control Signing and Key Management procedures.*

The terminal application will manage the software update and verify the signed files using RSA certificates, prior to the updates being downloaded. Unauthenticated files will be deemed unauthorised and will fail during authentication, resulting in terminal malfunction and make the terminal as unusable.[4]

[3] PCI PA-DSS requirements 3.1, 3.2, 9.1, 11.2 and 12.1.
[4] PCI PA-DSS requirements 10.2, 10.3.1 and 10.3.2

Please note: *Unauthenticated changes or updates to the application or its functions will not be permitted.*

Latest software/configuration updates will be available for download via WebCom. A PTID (Physical Terminal ID) is used to determine a software update, which will need to be flagged for download in WebCom (please refer to the WebCom manual for more details). Subsequently, log out and log back into the terminal to activate the download process, alternatively use 'Update Management' option within the setup menu.

PA-DSS Requirements: *There must be a secure delivery of remote payment application updates supported by remote access software.*

Please note: *PAYware Ocius utilises a challenge/response system to ensure application updates originate from Verifone's Terminal Management System (TMS).*

This secure, remote upgrade functionality reduces the burden of software upgrades and key management.

CONFIGURATION

This section outlines how to configure the different PAYware Ocius solutions. Although most menu structures are kept the same where possible, there are models which require different options, e.g. wireless connection details.

Verifone Support Application

In order to edit any of the settings files, the Verifone Support Application can be used to decrypt the files (please contact Technical Services department for more details). To open the file, either directly launch the application (located at: 'C:\Program Files\Commidea\Commidea Support Application\Commidea Support Application.exe') or open a .ccf file. A password prompt is then presented:

There is no default password required when logging in for the first time, the password box should be left blank before clicking 'Ok' to login. Use the 'Open' drop down menu and locate the file to be viewed.

Please note: *The Verifone Support Application password should be changed at the earliest opportunity by navigating to "File -> Settings", and amending the details within the 'Password' tab.*

When making changes to files, it is necessary to edit the field value and then select the row below before exiting the application. This registers the change that has been made and the user will be prompted to save changes before closing. If not request to save changes is polled, it should be presumed that the changes were not saved and will need to be remade.

Wireless Configuration

The PAYware Ocius VX 680 Wi-Fi terminal requires wireless network technology in order to function. When attempting to connect to a wireless network for the first time please ensure all vendor default passwords are changing appropriately.

The following security measures are recommended:

- Encryption keys should be changed from default at installation, and when anyone with knowledge of the keys leaves the company or changes positions.
- Default community strings must be changed.
- Default passwords/passphrases on access points must be changed.
- Firmware must be updated to support strong encryption for authentication and transmission over wireless networks.
- Other security-related wireless vendor defaults must be changed, where applicable.

Please refer to the additional PA-DSS guidelines below for wireless configuration:[5]

PA-DSS Requirements: *Wireless technology must be securely implemented and transmissions of cardholder data over wireless networks must be secure. Users must also change encryption keys and defaults passwords on access points.*

Please note: *It has been prohibited to use WEP for any new wireless implementations transmitting cardholder data since June 2010.*

[5] PA-DSS 6.1, 6.2 and 6.2b

PAYWARE OCIUS TERMINALS

There are Quick Reference Guides (QRGs) available for all terminal types to provide users with an overview of how to process transactions and perform everyday functions.

Out of the box, the terminals are pre-configured to communicate with the Gateway service. All available configuration options are covered in this section, however, in many cases it will not be necessary to make any changes on the terminal before starting to process transactions.

Plug the power cord into the terminal and power it on. A network connection will be required before transactions can be processed on the terminal, but this is not required for making configuration changes. This provides the ability to send terminals to site pre-configured correctly, where all the required details are to hand.

After an initial splash screen is displayed, showing the firmware version, the terminal will display the following:

1. Select ‘Setup’ on the screen, to enter the setup menu.

2. The Setup PIN will be requested, which is ‘2580’. Use the keypad to enter this value, and then use the **green** key or select the arrow on the screen to continue.

3. The Setup Menu is then presented.

As seen in the screen examples above, there are four sections to the Setup Menu:

1. **Network Settings**
   This section allows configuration of the transaction server, local server, terminal network settings, authorisation timeout and automatic update settings.

2. **Txn Settings**
   The Transaction settings control how the terminal reacts during transaction processing. Config ICC, enabling/disabling keyed transactions, PIN bypass and offline transactions are all configured within here.

3. **App Settings**
   The Application settings define how the software is set. PIN pad configuration, POS connection, surcharge, and manager PIN are all located within this section.

4. **Value Add Settings**
   This option allows configuration of the value-added services supported with the terminal, which may differ for different terminal types.

5. **System Info**
   A receipt containing all system information is printed on selection of this option. Information such as the PTID (displayed as Terminal ID) and App Version are listed.

All contained configuration options are detailed in the following subsections:

Network Settings

The table below shows which configuration options are available within this menu. Also shown are the settings available and a detailed explanation:

MENU OPTION	NEXT MENU OPTIONS	AVAILABLE OPTIONS AND/OR DESCRIPTION
1. Transaction Server	1. PAYware Ocius	Connect to Gateway servers for authorisation
	2. Local	Use a local WinTI for authorisation
2. Bill Manager	(Configuration only required if using a Bill Manager Server and only available on certain terminal types)	
	1. IP Address	Enter IP address of Bill Manager server
	2. Port	Enter Port to connect to Bill Manager on, (default value – 29000)
3. Terminal	Local Network settings for the terminal, used to provide a connection to the Gateway servers for transaction processing and/or account/software updates	
	1. Terminal IP	Enter IP address assigned to terminal on the network or 0.0.0.0 for DHCP
	2. Subnet Mask	Enter Subnet Mask of the network
	3. IP Gateway	Enter IP Gateway of the network
	4. Primary DNS	Enter Primary DNS of the network (if applicable)
	5. Secondary DNS	Enter Secondary DNS of the network (if applicable) To configure the terminal for DHCP, enter '0.0.0.0' for the Terminal IP, Subnet Mask and IP Gateway. The terminal will be configured in this manner by default.

4. Auth Timeout	Enter a value in seconds to define the timeout period during authorisation	
5. Update Management	1. All Updates	Automatically download all update types
	2. Prompt for Optional Updates	Ask user after login to “check for updates” for optional updates
	3. Mandatory Updates Only	Automatically download mandatory updates, do not check for others
(Next page) ***Depending on the Media Type utilised for VX 680, the applicable terminal network settings detailed below will be available as option ’1’***		
1 .BT Base Settings	Only available on VX 680 Bluetooth terminals	
	1. BT Base Scan	Scans all the base stations available within the bluetooth frequency range
	2. Reset BT Base	Removes existing base station settings from the terminal
1. Mobile Internet	Only available on VX 680 GPRS terminals	
	1. APN Details	1. Use Stored APN Details
		2.Use APN Manual Override
	2. APN Manual Override	1. APN
		2. User Name
		3. Password
	3. Operator Selection	1. Automatic
		2. Manual
		3. Preferred Network
1. WiFi Settings	Only available on VX 680 WiFi terminals	
	1. Channel	MUST be left ’blank’ to allow default WiFi configuration
	2. SSID	(Service Set Identifier) - a unique password to access a WiFi network point
	3. Encryption	1. None
		2. WPA
		3. WPA2

Please note: *Verifone cannot provide the local network settings required for option 3. ‘Terminal’, this would need to be acquired from your network administrator.*

Rather than having Primary DNS and Secondary DNS, there is ‘DHCP’ which provides the ability to choose between ‘Static IP’ and ‘DHCP’ when the terminal attempts to acquire an IP address on the network. Use ‘Static IP’ to preconfigure an IP address for the terminal, or DHCP for one to be dynamically allocated during connection.

Txn Settings

All available options for each menu are shown below:

MENU OPTION	AVAILABLE OPTIONS AND/OR DESCRIPTION
1. EMV Settings	1. Chip And Pin - connect to Gateway servers for authorisation
	2. Swipe Only – transactions are to be swiped using a magnetic strip reader
	3. None - used for cardholder not present scenarios
2. Keyed Transactions	1. Enabled - enable keying in of card details during a transaction
	2. Disabled - disable keying in of card details during a transaction
3. PIN Bypass	(Must be triggered by integration)
	1. Enabled - enable PIN code bypass
	2. Disabled - disable bypassing of card PIN code
4. Offline Txns	1. Enabled - enable storing of transactions offline
	2. Disabled - disable storing transactions offline
(Next page)	
1. ---	Reserved for future use
2. CTLS Receipt Settings	1. None
	2. Merchant
	3. Customer
	4.Both

App Settings

The configuration options for App Settings are all listed in the ensuing table:

MENU OPTION	NEXT MENU OPTIONS	AVAILABLE OPTIONS AND/OR DESCRIPTION
1. Integration	1. Integration	1. Use Socket Code
		2. COM1
		3. COM2
	2. Status Messages	1. Enabled
		2. Disabled
	3. POS Login Responses	1. Partial Responses – configure login responses to be returned to the POS
		2. Full Responses – enable full responses
2. Surcharge %	Enter a surcharge percentage to be added to each transaction (Default value – 0.00)	
3. Manager PIN	Enter the manager PIN, used for administrative operations (Default value – 5555)	
(Next page)		
1. Contactless Reader	Only available on terminals which support Contactless	
	1. Enabled – select this option to allow contactless payments of up to the value of £20	
	2. Disabled – select this option to disable the option to take payments via contactless reader	
2. Idle Card Read	1. Enabled - enable PAYware Ocius automatically starting a new transaction upon card insert	
	2. Disabled – disable this functionality	
3. Set Log Port	1. Disabled	
	2 COM1	
	3. COM2	
4. Screen Calibration	Allows the user to re-align the coordinates of the touch screen, by touching the points on the screen	

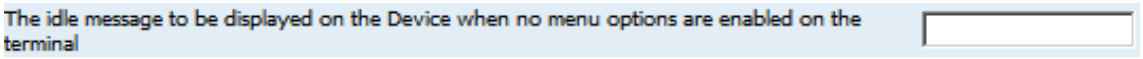
System Info

As mentioned above, choosing this option will produce a report of system information. This may be requested by the Merchant Helpdesk to acquire information on the version of terminal software running on the terminal (App Version), or the PTID of the terminal (Physical Terminal ID) which is usually found on the back of the terminal or under the battery.

Additional Settings – Terminal Configuration via WebCom

As new configuration options are added to PAYware Ocius; rather than releasing software updates to incorporate new menu items to allow them to be set, WebCom contains a 'Terminal Configuration' section which allows configuration profiles to be created.

For example, the functionality to add an idle screen message can be configured within WebCom, saved to a configuration profile which is then uploaded to the terminal.



For more information on this and other WebCom features, please see the latest version of the WebCom Manual. This is available via the 'View Help' link once logged in.

Auto Logoff

The auto logoff timeout functionality is used to log the current user off the terminal after a specific length of inactivity. The timeout is set to 120 minutes by default.

The ability to configure this timeout is currently not available in WebCom. To change the timeout value, please contact VeriFone Merchant Helpdesk team.

INTEGRATION

This section aims to inform the user of the options available to them to integrate into the PAYware Ocius Solution.

It will cover the different Integration Methods which can be utilised, and all record formats. Extra functionality for each solution will be provided in separate sub sections.

TESTING VALUES

To allow integrators to simulate responses which will need to be catered for within the integration, the following test values have been provided:

- Values ending in 2pence (e.g. £10.02) will simulate a Voice Referral
- Values ending in 5pence (e.g. £10.05) will simulate a Decline
- Values ending in 7pence (e.g. £10.07) will simulate 'Comms Down'

Communications Down ('Comms Down') is a scenario whereby the Gateway Managed service is unable to contact the Acquirer. This could be due to the Acquirer being down or due to x.25 issues.

During development, integrators can process transactions utilising the above values to ensure that their solution caters for all required scenarios.

INTEGRATION METHODS

In an effort to provide a solution to suit a broad range of clients, PAYware Ocius offers a couple of different Integration Methods:

Socket Connection

Socket connection integration is the most popular choice and method recommended by Verifone.

This method gives the most control over the system, and also provides the extra provision to install a system that has no on-site software requirements, avoiding some of the potential problems experienced by engineers in the field.

The socket connection will be ended by the terminal once the requested operation has completed, the integrator should never break the socket connection; otherwise, this will cause the transaction to be cancelled. If a socket connection is opened but no data sent down the socket within 20 seconds, PAYware Ocius will automatically disconnect the client.

Each record sent to the terminal must be terminated by a carriage return line feed (CRLF), unless configured otherwise within the software.

Each record received by PAYware Ocius will be acknowledged, by responding with an ASCII character of 0x06 (ACK).

RS232 Connection

The RS232 connection is generally used in a scenario where either the POS, or the programming language the POS software is written in, does not support TCP/IP. This results in the inability to

create a socket connection from the POS to the payment terminal, and hence the connection is established with the use of an RS232 cable. These cables are manufactured by Verifone and are available from Verifone. Alternatively, contact Verifone for a copy of the wiring diagram to manufacture your own.

The connection should be established using these settings:

NAME	SETTING
Baud Rate	9600bps
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Once the RS232 connection is made, the record is transmitted through the cable in exactly the same way as with a socket connection, but the CR/LF pair is not required.

On PAYware Ocius Terminals, a **socket connection** should be established to port 25000, and a record then passed down the socket connection. This will need to be terminated by a CR/LF pair.

If **text files** are used for integration, these will have to be passed to a Bill Manager server and then forwarded onto the terminal.

All possible records that can be sent to the terminals are covered in section 13.6, along with an explanation of the use of each type.

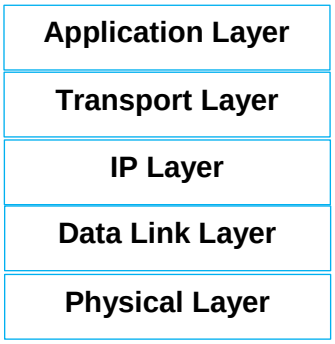
[6]

Please note: *Merchants must ensure they use the secure protocols included within this guide when using Verifone's approved PAYware Ocius software and supported terminals. Use of any other protocols is not supported (PA-DSS 5.4)*

IP Stack

The TCP/IP connection provides end-to-end connectivity, specifying how data should be packaged, addressed, transmitted, routed and received at the destination. The connection is organised into layers known as IP stack, which are used to organise all related protocols according to the scope of networking involved.

The following IP stack model is used within the PAYware Ocius terminal solution:



[6] PA-DSS 5.4

The physical and data link layers contain the link between the terminals and/or POS systems for a single network link. When a transaction is initiated via socket connection, communication is transmitted using the TCP and IP layers, interconnecting the hosts across independent networks and communicating data to the applications.

The terminal application implements the Application Layer of the protocol stack described above using the API that the underlying Transport Layer (i.e. TCP) exposes. The terminal application does not override or circumvent functions of any of the underlying layers in any way.

Please note: *The PAYware Ocius terminal solution uses defined set of P2PE approved IP stack and only IP stack approved as part of the PTS review is used.*

TRANSACTION PROCESSING

By establishing a connection to the terminal directly, a transaction can be passed to the PAYware Ocius terminal. On receiving a T Record, the PAYware Ocius terminal begins the card processing cycle. Once the transaction has been completed, an output response is returned, detailing the result of the transaction. All output records are terminated by a CR/LF pair.

RECEIPTS

PAYware Ocius terminals are generically certified within the UK and as such the receipts produced form part of the accreditation – the contents and layout are all predetermined.

Please note: *When making changes to receipts, even from an existing integration which has been certified by Verifone, that it is necessary to contact Technical Services for re-approval.*

Voucher Record

When configured accordingly, it is possible to enable Voucher Records to be sent from the terminal to the POS in order to print the vouchers on a local printer. The functionality can be enabled by amending a terminal setting named ‘POS Voucher’.

Enabling the voucher record functionality will not disable any voucher printing on the terminal via the integrated thermal printer (ITP); therefore should the merchant no longer wish to print using this method should remove the tally roll from the terminal, or discard the vouchers once printed.

Should the need arise to reprint then the ‘REP,101’ command can be used to print the last customer receipt.

The Voucher Record provides the ability for the terminal to export the voucher (also known as receipt) information via an integrated message to the POS, allowing use of an external printer rather than the terminal’s integrated thermal printer (ITP).

The record consists of a variable number of comma separated fields, with the first field being populated with a ‘V’ to denote the message type.

The remaining fields will comprise the data that would be printed on the ITP, with each line represented as a single field. Any formatting codes, leading and trailing spaces used on the ITP will be omitted from the Voucher Record.

The length of the record will depend upon the content, e.g. how many lines the merchant has their voucher header configured to. By way of example, here is a table to show a record with and a record without a voucher header:

FIELD	WITH HEADER	WITHOUT HEADER
1	V	V
2	*** MERCHANT COPY ***	*** MERCHANT COPY ***
3	Verifone Ltd	Visa
4	Visa	492912*****23
5	492912*****23	Expiry: 12/10
6	Expiry: 12/10	...
8	...	

Please note: *Acquirer accreditation will be required for any merchant wishing to use the XML receipt option. The only exception to this being; if the XML receipts are built to exactly represent the text file format.*

Please contact Technical Services if you have any queries on this - no solution using XML receipts will be passed for live processing until the acquirer confirmation is gained.

RECORD FORMATS

All possible record formats are detailed within this section, giving an understanding of how it is possible to customise an integration to suit the customer requirements.

Each record sent to the terminal must be terminated by a carriage return line feed (CRLF), unless configured otherwise within the software.

Account Check Transaction Type

Within the transaction request message, field 3 *txntype* is used to define the transaction type. The following transaction types are available:

- 01 – Purchase
- 02 – Refund
- 07 – Account Check

The Account Check transaction type service is used in conjunction with Card Verification Code (CSC) and Address Verification Service (AVS), allowing merchants to validate a card account for debit and prepaid services without impacting the cardholder's funds.

Account check is mandated by Visa and MasterCard to supersede Verifone's existing Authorisation Only (Auth Only) process, which uses a nominal value to validate an account.

The transaction type does not indicate whether funds are available on the account. It is primarily used to confirm that the account exists and is not blocked or invalid.

To process an Account Check transaction via integration, the *txntype* field needs to be configured to '07' and the value must be presented with a '0.00' value.

The Account Check authorisation result will be confirmed as either “Account Valid” or “Cannot Validate” within the *authmessage* (authorisation message) field depending on the transaction result returned within the transaction response message:

- If the *txnresult* returns “Declined” – the *authmessage* (authorisation message) will return “CANNOT VALIDATE”.
- If the *txnresult* returns “AuthOnly” – the *authmessage* (authorisation message) will return “ACCOUNT VALID”.

Please note: *Due to the nature of the service, the transaction does not require confirmation.*

Type Definition Change

Existing PAYware Ocius integrators may recognise a change in the message format specifications with regard to the description of field lengths.

There are an increasing number of occasions where the length of the data is changing beyond Verifone’s control, particularly with regard to the Card Scheme label in field 13 of the transaction output message.

For this reason, Verifone have been forced to remove the guidelines surrounding maximum field lengths for the output records.

TRANSACTION REQUEST (T RECORD)

Detailed below is the format of the most frequently used record, the Transaction Record. This is used for initiating transactions on the terminal.

It is followed by the resultant output response generated after the transaction record has been processed. The appropriate version of the response message will be automatically selected by the terminal depending upon the information included with the transaction request.

The transaction request message must conform to the below standard:

FIELD	NAME	TYPE	DESCRIPTION
1	Message Type	String Mandatory	'T' to be passed, to define a transaction record
2	Account Number		This field is no longer used. Field 24, Account ID, is used to define the merchant parameter set to use
3	Transaction Type	Integer Mandatory	'01' – Purchase '02' – Refund '07 – Account Check'
4	Modifier	Integer Mandatory	The modifier meanings have been updated to account for the different types of CNP transactions: '0000' – Cardholder Present '0002' – Offline (Capture) '0004' – Online '0008' – CNP – Mail Order '0010' – Authorisation Only '0020' – Continuous Authority '0200' – Electronic Commerce '1000' – CNP – Telephone Order '2000' – CNP – Account On File
5	PoS Routing / Bill ID		Reserved, leave empty
6	PAN / Track 2		Reserved, leave empty
7	CSC		Reserved, leave empty
8	Expiry Date		Reserved, leave empty
9	Issue No		Reserved, leave empty
10	Start Date		Reserved, leave empty
11	Txn Value	Decimal Mandatory	Total value of the transaction including tax applies to: Purchase, Refund, Cheque Guarantee, Cash Advance and Purchase with Cash Back (PWCB). In the case of PWCB transactions, this field should only contain the values of the goods or services provided. Provision of the decimal point is recommended although optional. For example: 1.23 = £1.23 123=£123.00, 000001.2389 = £1.23. Values should always be positive, and will be truncated to the correct number of decimal places required for the currency. For example: 1.23 = 1¥ (one Japanese Yen) (0 decimal places)).
12	Cash Back Value	Decimal Conditional	Total Cash Back Value for Purchase with Cash Back transactions (PWCB). Values will be truncated (without rounding) to the number of decimal places required for the given currency. The value should always be positive. If left blank, the terminal will prompt for cashback. If populated with a value, or zero value, the terminal will not prompt.
13	Bank Acc No		Reserved, leave empty
14	Sort Code		Reserved, leave empty
15	Cheque No		Reserved, leave empty

16	Cheque Type		Reserved, leave empty
17	Cardholder Name		Reserved, leave empty
18	Cardholder Billing Address		Reserved, leave empty
19	EFTSN		Reserved, leave empty
20	Auth Source		Reserved, leave empty
21	Auth Code		Reserved, leave empty
22	Txn Date Time		Reserved, leave empty
23	Reference	String Optional	Reference numbers can be supplied up to a maximum length of 50 characters. When forwarded to the acquirer these are truncated to 25 characters
24	Account ID	Decimal Optional	Defines merchant parameter set to be used
25	Gratuity	Decimal Conditional	Total gratuity value to be added to the transaction. Provision of the decimal point is recommended although optional. For example: 1.23 = £1.23 123=£123.00, 000001.2389 = £1.23. Values should always be positive, and will be truncated to the correct number of decimal places required for the currency. For example: 1.23 = 1¥ (one Japanese Yen) (0 decimal places))
Fields 26, 27 & 28 are available with the PAYware Ocius Vx Range from version V03.02.38.xxxxx onwards. Prior versions require a 25 field transaction record			
26	NDI Value	Decimal Conditional	Non Discounted Items value, showing the value of items which are not eligible for Freedom. This field is conditional, as it will only be populated if there are values meeting this criterion.
27	Register for Account On File	Integer	Valid values are: Not Set = 0 Do Not Register = 1 Register = 2 Register Only = 3
28	Token ID	Decimal	ID assigned to the stored Account On File details

TRANSACTION RESPONSE (INITIAL)

FIELD	NAME	TYPE	DESCRIPTION
1	Result	Integer	Transaction result: '0' – Completed '7' – Declined '100' – Status Message '-nn' – All other negative values are used to define error conditions Appendix A contains a full list of error codes and messages. Screenless and UPT transaction results: '0' – Completed '2' – Referred '5' – Declined '6' – Authorised '7' – Reversed '8' – Comms Down '-nn' – Negative values are used to define error conditions
2	Terminate Loop	Integer	Reserved, Ignore
3	Total Transaction Value Processed	Decimal	Values will be truncated to the correct number of decimal places required for the transaction currency. For example: 1.23 = 1 (one Japanese Yen) Field will show total that will be debited, inclusive of any DCC.
4	Cashback Value	Decimal	As above
5	Gratuity Value	Decimal	As above
6	PAN	Decimal	A copy of the PAN field from the .in file (if card details are keyed) or the PAN derived from Track2/ICC. Please note: This value will not be returned in full due to PCI requirements.
7	Expiry Date MMYY	Decimal	Card Expiry Month and Year.
8	Issue Number	Decimal	Card Issue Number. Blank when scheme does not provide an issue number.
9	Start MMYY	Decimal	Card start month and year
10	Transaction Date / Time	Decimal	CCYYMMDDHHMMSS
11	Merchant Number	Decimal	The Merchant Number for the given card scheme and account.
12	Terminal ID	Decimal	Terminal ID used for this transaction.
13	Scheme Name	String	Card scheme name **Please note: American Express ExpressPay contactless transactions are not supported*
14	Floor Limit	Decimal	Floor limit for the card scheme/account.
15	EFT Sequence Number	Decimal	Four digits in the range 0001 – 9999. (Prefixed with "OL" when offline)
16	Authorisation Code	String	Blank if the transaction is declined or is below the floor limit.
17	Referral Telephone Number.	Decimal	Used to return the voice referral phone number when in Screenless/UPT modes
18	Customer Verification Method / Authorisation Message / Error Message / Status Message	String	As returned by communications process. Normally direct from acquirer. Also contains status message if enabled

TRANSACTION RESPONSE (VERSION2)

FIELD	NAME	TYPE	DESCRIPTION
First 18 fields are the same as **Transaction Output Record (Initial)**			
19	Capture Method	String	Valid values are: Contactless Swipe ICC Keyed
20	Transaction Currency Code		Currency Code associated with the transaction
21	Original Transaction Value		Transaction value based on the original base currency
22	Original Cashback Value		Cashback value based on the original base currency
23	Original Gratuity Value		Gratutiy Value based on the original base currency
24	Original Transaction Currency Code		Currency code associated with the base currency
25	Barclaycard Freedom Discount Value (ceased)		Value of discount received due to Barclaycard Freedom scheme
26	Barclaycard Freedom Redemption Value (ceased)		Value of Barclaycard Freedom Reward Money redeemed during the transaction (i.e. Reward Money earned from previous transactions which have been used to pay for the current transaction)
27	Account on File Registration Result	Integer	This is the result of the Account on File registration. Valid values are: '0' – Not Set '1' – Not Performed '2' – Success '3' – Failed
28	Token ID	String	This is the token allocated to the payment details as part of the Account on File registration process or the token used for the Account on File payment.
29	AVS Post Code Result	Integer	This is the result of any AVS post code checking. Valid values are: '0' – Unknown '1' – Not Checked '2' – Matched '4' – Not Matched '8' – Reserved
30	AVS House Number Result	Integer	This is the result of any AVS house number checking. Valid values are: '0' – Unknown '1' – Not Checked '2' – Matched '4' – Not Matched '8' – Reserved
31	CSC Result	Integer	This is the result of any CSC verification. Valid values are: '0' – Unknown '1' – Not Checked '2' – Matched '4' – Not Matched '8' – Reserved

TRANSACTION RESPONSE (VERSION3)

FIELD	NAME	TYPE	DESCRIPTION
Fields 19 to 31 are the same as transaction output record (version2)			
32	Card Number Hash	String	This is the hash of the card number that is generated by the WinTI3 infrastructure.

TRANSACTION RESPONSE (VERSION4)

FIELD	NAME	TYPE	DESCRIPTION
Fields prior to 33 are the same as Transaction Output Record (Version3)			
33	VGIS Reference	String	This is the VGIS reference if a VGIS transaction has been processed.

TRANSACTION RESPONSE (VERSION5)

FIELD	NAME	TYPE	DESCRIPTION
Fields prior to 34 are the same as Transaction Output Record (Version4)			
34	Track1 Discretionary Data	String	Data captured from the Track1 Discretionary Data field, e.g. Loyalty Card Number

TRANSACTION RESPONSE (VERSION6)

FIELD	NAME	TYPE	DESCRIPTION
Fields prior to 35 are the same as Transaction Output Record (Version5)			
35	CharityDonationValue	Decimal	The donation value which has been incorporated as part of the transaction value
36	CharityDonationMerchantNumber	String	The charitable donation provider allocated merchant number
37	OriginalCharityDonationValue	Decimal	The donation value which has been incorporated as part of the transaction value prior to currency conversion being performed (if applicable)

TRANSACTION RESPONSE (VERSION7)

FIELD	NAME	TYPE	DESCRIPTION
Fields prior to 38 are the same as Transaction Output Record (Version6)			
38	Transaction Id	Decimal	This is the ID of the transaction assigned by the hosted service.
39	Authorisation Server Name	String	This is the name of the authorisation server that processed the transaction.

TRANSACTION RESPONSE (VERSION8)

FIELD	NAME	TYPE	DESCRIPTION
FIELDS PRIOR TO 40 ARE THE SAME AS TRANSACTION OUTPUT RECORD (VERSION7)			
40	Card Scheme ID	Decimal	This is the ID of the card scheme

Example message (40 fields):

0,1,10.00,0.00,0.00,**********0002,0308,,0402,20121212152308,22048042,28200005,Visa,,2206,060377,,PIN VERIFIED,ICC,826,,,,,,1,,0,0,0,SFJtHyYqGFm0r4ksPY6vGTE9x9s=,,,0.00,,,108112,AuthDB\RND-DB-1,2,

L2 RECORD

An L2 record can be used to stipulate which menu structures are enabled for the operator. Here's a description of this record type:

FIELD	NAME	TYPE	DESCRIPTION
1	L2 (Upper Case)	String *Mandatory*	'L2' – Indicates an L2 format Login Record
2	UserID	String *Mandatory*	User ID
3	PIN	String Mandatory	User PIN
4	Menu Options	String *Conditional*	See Menu list in table attached below

FIELD	MENU OPTION
'1'	New Transaction
	[Not possible to restrict sub menus. This is controlled by Account Permissions]
	Menu
	'1' – Transaction Management
	'1' – Reports
	1. Terminal '1' - Z Report '2' - X Report '3' - Txn Report '4' - Q Report '5' - Offline Transactions '6' - Stored Offline Transactions 2. Account '1' - Account Summary '2' - Account details '3' - End of Day 3. Bank Report 4. Last Printed Report
	'2' . Submit Offine Transactions
	'2' - Reprint
	'3' – System 1. Print Stored AID's 2. System Info 3. Voucher Type 4. Change Setup Pin
	'4' - Ordering 1. Get Order List 2. Place Order
	'5' - User Management 1. Add New User 2. Change User ID 3. Change User PIN
	l Management (options vary depending on terminal/software) 1. Power 2. Reboot Pinpad

	3. Signal Strength
	Bill Options 1. Close Bill on POS 2. Get Bill 3. Get/Print Bill 4. Print Bill
	Logoff
	Other 1. Nectar 2. E-Top-up 3. Givex 4. MVoucher

The menu allows for the menu options available to be listed by placing all the required options in the fourth field of the record. For example, to include all the menus and their sub-menus (for a user with a Login ID and PIN of 1234):

L2,1234,1234,*

For more specific configurations, it is possible to only enable the operator access to the logout option. This would be achievable using the following record:

L2,1234,1234,4

By including a 4, none of the other options are accessible.

Leaving the fourth field blank would specify that no options would be available at all, rendering the application completely controlled by records from the POS.

To control the sub menus as well a set of "{ }" must be included after the option selected, and within the brackets list which sub options are utilisable. An example here would be where Select Bill is required, but only Print Bill to be available within the sub menu (option 4 of the four sub-options):

L2,1234,1234,3 {4} 4

As with the previous example, for all sub options to be available then include {*} after the option. Not including anything will only allow the top menu to be accessed. The only exception to this rule is the New Transaction option, which is controlled using the permissions setup on the account.

Please note: *It is also possible to control a user's menu options by configuring a 'Permission Profile' within WebCom. For instructions on how to do this, please see the WebCom manual.*

LOGOUT RECORD (O-RECORD)

The terminal Logout command has now been updated to the following:

FIELD	NAME	TYPE	DESCRIPTION
1	O (Upper case)	String *Mandatory*	'O' – Indicates Logout Record
2	Function	Integer *Mandatory*	'0' – Logout '1' – Print Q Report and logout

A final response is sent once the action has been processed, informing the operator of the outcome. Similarly to the login record, a '0' record is received back to confirm a successful logout, or a '-31' for a processing error. If attempting to logout when there is no user logged in, a '-85' error message is received.

POS PROGRESS MESSAGE/CUSTOMER FACING MESSAGES

To provide information on the status of a transaction, status messages can be enabled on the terminal. These will report the progress of the terminal at the appropriate stage.

This feature is enabled by a configuration download but disabled by default. It will result in status messages being outputted by the terminal in the same format as standard integration messages, with a result code of '100'.

The messages will be outputted in the following scenarios:

- Authorising
- Card inserted
- Card swiped
- Cardholder print complete
- Checking signature
- Confirming
- Getting PIN
- Low Signal Strength
- Merchant print complete
- NO SIM CARD
- Unable to connect to server
- Voice Referral required

The POS Progress Message is sent to the POS via a socket connection (set to port 25001 by default). This message is utilised to inform the POS of the status of the transaction.

FIELD	NAME	TYPE	DESCRIPTION	
1	Result	Integer	This indicates the result code (100)	
2	Terminate Loop	Integer	Reserved, Ignore	
3	Status ID	Integer	This indicates the progress status. Below is a list of all possible outcomes: (* denotes not applicable for UPT transactions)	Suggested on screen message to display to customer for each status: (depending upon Screenless/UPT)
			ProcessingTxn = 0	"Please Wait"
			*WaitingForGratuity = 1	"Enter Gratuity"
			*GratuityBeingEntered = 2	No message required [Informs POS that the gratuity is being entered on screen]
			AwaitingCard = 3	"Present Card" / "Insert Card"
			SwipeCard = 4	"Swipe Card" / "Remove Card"
			CardInserted = 5	"Please Wait"
			CardRemoved = 6	"Please Wait"
			CardProcessing = 7	"Do Not Remove Card"
			ChangeCard = 8	"Use Alternative Payment Method"
			ContactTxnRequired = 9	"Insert Card"
			*KeyInCardDetails = 10	"Key Card Number"
			*WaitingForCashback = 11	"Enter Cashback"
			PinEntry = 12	"Enter PIN"
			RiskManagementComplete = 13	No message required [Informs POS that PIN has been entered/stage where PIN would be entered has been completed]
			AuthorisingTxn = 14	"Please Wait"

	WaitingForResult = 15	“Please Wait”
	AuthResultReceived = 16	“Please Wait”
	PrintingReceipt = 17	“Please Wait”
	*SignatureConfirmation Required = 18	“Please Wait”
	ContinueRequired = 19	No message required [Informs POS that PAYware Ocius requires information to continue – see ‘Continue Transaction Record’ section
	*ConfirmAuthCode = 20	Display all the information on screen to allow a Voice Referral to be processed; Merchant Number, Correct Bank Telephone Number and all transaction details
	ConfirmingTxn = 21	“Please Wait”
	RejectingTxn = 22	“Declined”
	FinalResultReceived = 23	“Please Wait”
	*VoiceReferral = 24	“Referral”
	RemoveCard = 25	“Remove Card”
	AuthResultError = 26	“Unable To Authorise”
	FallbackToSwipeDisabled = 27	“Not Accepted”
	DownloadingFile = 28	“Loading”
	UpdatingPED = 29	“Loading”
	InvalidPEDConfig = 30	No message required [Informs POS that there is a PED Config error]
	CardDataRetrieval = 31	“Please Wait”
	StartingTransaction = 32	“Please Wait”
	PerformingDownload = 33	“Loading”
	RequestingReport = 34	“Please Wait”
	*GratuitySelectionRequired = 35	“Gratuity? Enter/Cancel”
	ExpiryDateRequired = 36	“Expires MM/YY”
	StartDateRequired = 37	“Valid From MM/YY”
	IssueNumberRequired = 38	“Issue Number”
	AVSHouseNumberRequired = 39	“Enter House Number”
	AVSPostCodeRequired = 40	“Enter Post Code”
	CSCRequired = 41	“Enter Card Security Code”
	*CustomerPresentNotPresent SelectionRequired = 42	“Customer Present? Yes/No”
	*CustomerNotPresentOption SelectionRequired = 43	“Select Transaction Type: 1. E-Commerce 2. Mail Order 3. Telephone Order”
	EnterChargeAuthCode = 44	“Enter Charge Auth Code”
	LoginRequired = 45	No message required [Informs POS that PAYware Ocius is ready to be logged in]
	Ready = 46	“Ready”
	CardNotAccepted = 47	“Not Accepted”
	CardBlocked = 48	“Not Accepted”

			TransactionCancelled = 49	“Transaction Void”
			*InvalidExpiry = 50	“Not Accepted”
			*GrauityInvalid = 51	“Gratuity Amount Invalid”
			InvalidCard = 52	“Invalid Card
			PrintingCustomerReceipt =53	“Please Wait”
			InitialisingPED = 54	“Please Wait”
			PEDUnavailable = 55	No message required [Informs POS that the PED is unavailable]
			CardAppSelection = 56	“Select Payment Type”
			RetryDownload = 57	No message required
			RestartAfterSoftwareUpdate = 58	No message required
			RequestingDCC = 59	“Please Wait”
			*****DCCCurrencyChoice = 60	No message required
			CardholderDCCCurrencyChoice = 61	“Please select currency” [include details of currency options]
			UnsafeDownload = 62	No message required
			UnexpectedLogin = 63	No message required
			StartBarclaysBonusTxn = 64	No message required
			UpdateBarclaysBonusTxn = 65	No message required
			CancelBarclaysBonusTxn = 66	No message required
			ConfirmGratuity = 67	“Please confirm Gratuity amount”
			RegisterForAccountOnFileDecision = 68	No message required
			*****AwaitingTokenID = 69	No message required
			BBDiscountSummary = 70	“Discount Summary” [include summary details]
			BBUseBonus = 71	“Use Bonus – Yes/No”
			BBEnterRedemption = 72	“Enter Redemption Amount”
			BBNotAvailable = 73	“Not Available”
			DownloadComplete = 74	No message required
			DownloadStillBeingPrepared = 75	No message required
			ServerConnectionFailed = 76	No message required
			ResumeDownload = 77	No message required
			ReprintComplete = 78	No message required
4	Status	String	This is a text representation of the progress status	
5	Parameters	String	This field will contain any information that the POS may require that is associated with that status. Each parameter will be ‘;’ delimited and will be defined as follows: <Name>=<Value> Here is a list of all possible parameters: TXN VALUE CASHBACK VALUE GRATUITY VALUE TOTAL AMOUNT AUTH CODE VR TEL NO CARD EXPIRY MID TID FILENAME	

			PROGRESS SCHEME ID MERCHANT NAME

Stay Offline Request

The Stay Offline request is used to instruct the terminal to stay offline for a given length of time and not perform connection checks when starting a transaction.

FIELD	NAME	TYPE	DESCRIPTION
1	Message Identifier	String Mandatory	This identifies the type of message. This will always be 'STAYOFFLINE'
2	Option Identifier	Integer Mandatory	'0' – Online '1' to '98' – Stay offline for x minutes (minimum of 1, maximum of 98) '99' – Stay offline until the end of the day

Example message: STAYOFFLINE,20

Stay Offline Response

FIELD	NAME	TYPE	DESCRIPTION
1	Status ID	Integer Mandatory	Result of the request. Possible values are: 0 = Stay offline configuration complete
2	Terminate Loop	Integer Mandatory	This indicates whether the response is the last message for the associated command. Valid values are = 0 or 1 (Last Message)
3	RFU	N/A	Reserved for Future Use
4	RFU	N/A	Reserved for Future Use
5	RFU	N/A	Reserved for Future Use
6	RFU	N/A	Reserved for Future Use
7	RFU	N/A	Reserved for Future Use
8	RFU	N/A	Reserved for Future Use
9	RFU	N/A	Reserved for Future Use
10	RFU	N/A	Reserved for Future Use
11	RFU	N/A	Reserved for Future Use
12	RFU	N/A	Reserved for Future Use
13	RFU	N/A	Reserved for Future Use
14	RFU	N/A	Reserved for Future Use
15	RFU	N/A	Reserved for Future Use
16	RFU	N/A	Reserved for Future Use
17	RFU	N/A	Reserved for Future Use
18	General description	String Mandatory	Result message

Example message: 0,,,,,,,,,,,,,,,,,Stay Offline Configuration Complete

ADDITIONAL INTEGRATION COMMANDS

In order to provide extra functionality, the below commands are available. They can be used with any of the integration methods:

OUTPUT MESSAGE	DESCRIPTION
OLS,	On receipt of this integrated function, PAYware Ocius will submit all offline transactions and respond with a message informing the operator of the outcome. N.B. if the terminal is offline when OLS is sent, then a reconnection attempt will be made. If this fails, an error message of -87 will be sent to inform the POS of this result.
REP,x	Report command which when sent to PAYware Ocius for PC will produce a report, where x is the report required. Another variable; y (optional) can be supplied to provide the full filename to output the report to. Here are the reports available (x): '1' – **Z Report** – report detailing all transactions since last Z report run '2' – **X Report** – report detailing all transaction since last Z report, but without resetting the values as with Z report '3' – **Txn Report** – report of last 10 processed transactions '5' – **Q Report** – quick report showing total processed amount since last Z report, and the date and time of the last Z report '10' – **Last Printed Report (Re-print)** – reprints the last printed report '11' – **Stored Offline Txn** – report of any stored offline transactions which are yet to be submitted to the Gateway server '100' – **Product List** – prints a list of available products, e.g. till roll '101' – **Reprints customer receipt** – reprints customer receipt of the last processed transaction '103' – **Prints System Information report** – prints System Info report, which contains information about the software running on the device as well as all the network settings for the terminal '201' – **Live Store** – prints a report showing all transaction in the live store waiting to be sent for settlement '202' – **Session Report** –prints a report showing all transactions processed during the current logon session '203' – **Summary Settlement Report** – prints a report showing the totals, broken down by card scheme, of transaction from the last time the account was settled '204' – **Detailed Settlement Report** – prints a report showing each settled transaction included in the last settlement (e.g. the night before). '205' – **Barclays Gift Report** – prints report on all Barclays Gift transactions
REQINFO,x	Report produced containing requested information from a terminal, or an estate of terminals, depending on how the message is sent. Here are the commands that could be sent with the function: '1' – Returns the PTID of the terminal '2' – Software version on the terminal '3' – Login status report '4' – Displays "Please wait", and performs connection test to transaction server '5' – Returns the status of the PED from the last check performed by PAYware Ocius
UPDAPP,	This function will check for updates. Once the updates are completed, the standard response will be sent to the POS with details of download being successful 'Download Successful: x,x,x,x,x' where x details which downloads are performed. If a restart is required the message will read 'Download Successful & Restart Required: x,x,x,x,x'. If the update fails, then PAYware Ocius will return to the main menu, and the only situation when this is not the case is where the terminal is exited following a software update, and it will then need to be re-launched.
REQLASTMSG,	Returns the last message sent to the POS. If no message is stored, the following response is returned: "90,1,,,,,,,,,,,,,,,,Service Not Allowed"

ADDITIONAL FUNCTIONALITIES

Verifone offer merchants with additional functionalities to further enhance transaction processing and provide additional security when processing payments.

CASHBACK & GRATUITY

When enabled on a merchant account, cashback can be offered to a cardholder. This functionality can be integrated into the POS and, using the transaction record, pre-populated.

The cashback and gratuity fields within the transaction record are conditional, as they can only be supported if enabled on the account. If enabled, there are three options with regards to the fields, which apply to both cashback and gratuity:

- **Not to supply a value within the transaction record -** When the feature is enabled, not supplying a value will result in PAYware Ocius prompting the user for an amount on screen during the transaction if the card supports it.
- **Supply a value of '0' -** PAYware Ocius will not prompt for values for either and will assume that the functionality is not required (no cashback/gratuity).
- **Supply the value to be used -** If passed within the transaction record, the value will be automatically known by PAYware Ocius and will be added to the total transaction amount.

Please note: *If the functionality is disabled and the field within the transaction value is populated, then this will generate an error.*

GRATUITY WARNING LEVEL CHECK

If gratuities are being accepted on the account, it may be beneficial to make use of the gratuity warning level check functionality.

This allows a percentage value to be configured within WebCom, and if the gratuity amount to be added to the transaction is higher than the maximum percentage, then a warning is produced on screen.

For example with a transaction for £1 and the gratuity check set to '25' (25%), and then if the gratuity value was any higher than 25p, a warning would be displayed.

POST CONFIRM REVERSAL

The reversal functionality makes it possible to reverse a transaction after it has been completed but not submitted. This can be performed instead of a refund transaction. The Verix V terminals support the initiation of reversals in both integrated and standalone modes.

In standalone mode, the 'Reverse Last Transaction' option can be found under the 'TXN Management' sub-menu of the terminal's Main Menu screen. Once the reversal is completed, a transaction VOID receipt will be generated for the merchant and the customer.

In integration mode, the POS can send the following integration message: PCNFREV,

Upon completion of the reversal process, the terminal will inform the POS of the result, which will be sent in the following message format:

FIELD	NAME	TYPE	DESCRIPTION
1	Result	Integer	This indicates the result of the reversal. The following values are valid: '-ve' - Processing Error '0' – Successful '1' – Reversal Not Possible '2' – Transaction Already Reversed
2	Reversal Method	Integer	This indicates the method used to reverse the transaction. The following values are valid: '0' – Not Set '1' – Standard Reversal '2' – Refund
3	Transaction ID	Decimal	This is the transaction ID of the transaction that was requested to be reversed. Default = '-1' (Unknown)
4	Transaction Value	Decimal	This is the transaction value of the transaction that was requested to be reversed. Default = '0'
5	Cashback Value	Decimal	This is the cashback value of the transaction that was requested to be reversed. Default = '0'
6	Gratuity Value	Decimal	This is the gratuity value of the transaction that was requested to be reversed. Default = '0'
7	Starred PAN	String	This is the starred PAN of the transaction that was requested to be reversed. Default: Empty field
8	Transaction Date/Time	String	This is the transaction date/time of the transaction that was requested to be reversed. This is in the format: yyyyMMddHHmmss Default: Empty field

Example response for a successful post confirm reversal:
0,1,577985,10.00,0.00,0.00,492912******3127,20140527113233

Example response for a failed post confirm reversal:
1,0,-1,0.00,0.00,0.00,,

TRANSACTION STATUS MESSAGES

To provide information on the status of a transaction, status messages can be enabled. These will report the progress of the terminal at the appropriate stage.

This feature is enabled by a configuration download but disabled by default. It will result in status messages being outputted by the terminal in the same format as standard integration messages, with a result code of '100'.

The messages will be outputted in the following scenarios:

- Authorising
- Card inserted
- Card swiped
- Cardholder print complete
- Checking signature
- Confirming
- Getting PIN
- Low Signal Strength
- Merchant print complete
- NO SIM CARD
- Unable to connect to server
- Voice Referral required

ACCOUNT ON FILE

Account On File (also known as Tokenisation) enables merchants to store card payment details, which generates a 'token ID'. This unique reference to the details ensures that the merchant can link the token ID to the cardholder's details within the host system, and for recurring payments with the customer in question all that needs to be supplied to perform a transaction is the token ID.

In order to perform an Account On File transaction, the cardholder's payment details must first be registered. PAYware Ocius supports registering card details using two functions: Registration and Payment, or Registration only.

Both functions capture the details using an EFT transaction flow via any capture method other than Contactless.

Registration and Payment

This registration mechanism allows the merchant to perform a standard transaction whilst also storing these details for future 'Account On File' payment transactions.

The merchant performs a standard purchase or refund transaction in the normal fashion. If the merchant system is configured to support 'Account on File' and PAYware Ocius is operating in Online Mode, PAYware Ocius will prompt the user to make for their decision on account registration. This prompt occurs after the "Merchant Reference" prompt (again, if configured). After the decision has been made, standard transaction processing will continue.

When processing a transaction via integration, with 'Account on File' enabled, the decision on registering the details can be specified within the transaction record using field 27. See the transaction record definition for full details on the options available.

Prior to the transaction being sent for authorisation, PAYware Ocius will submit the payment details for 'Account on File' registration. After completion of the 'Account on File' registration process, standard authorisation processing will continue. Upon completion of the authorisation processing, PAYware Ocius will include the 'Account on File' registration details on the receipts.

Upon completion of the transaction, if the transaction is integrated, PAYware Ocius will return the integration response with additional fields added providing the token registration result details.

Registration Only

This registration function allows the merchant to store the cardholder's payment details for 'Account on File' payment transactions without processing any form of authorisation.

This registration mechanism is initiated by starting a modified transaction, either by selecting the customer present modifier or the customer not present modifier. PAYware Ocius will then follow a standard transaction flow. However, PAYware Ocius will automatically set the transaction value to 0.00, and skip the decision prompt for whether to perform the registration process.

At the point where a transaction would normally be authorised, PAYware Ocius will perform the registration process as defined in the 'Registration and Payment' function. Instead of sending the transaction for authorisation, PAYware Ocius will automatically decline the transaction locally, and complete as a registration only transaction.

As the transaction is registration only, PAYware Ocius will print receipts tailored for this type of transaction. At no point in this process are any payments attempted to be authorised.

Upon completion, if the transaction is integrated, PAYware Ocius will return the integration response with additional fields providing the Account on File registration result details.

Account on File Registration Validity Period

Payment details registered using the 'Account on File' mechanism will only be valid for a finite period of time. This time period is based upon 'Account on File Validity Period' configured against the merchant's system. The 'Account on File Validity Period' is defined in days.

Account On File Payment

Account on File payment is a Cardholder Not Present transaction type. As such, it can be initiated by selecting the corresponding Purchase or Refund option on the Customer Not Present transaction type screen.

PAYware Ocius will then process the transaction as normal. Upon processing the requested transaction, the terminal will request the token ID rather than card details. Within an Integrated environment, the token ID can be supplied within the Transaction Record.

The transaction processing will continue by submitting the transaction to the Gateway Service for authorisation. The Gateway Service will retrieve the relevant cardholder details from its database of registered cards, in order to perform authorisation.

PAYware Ocius will complete the transaction in a similar manner to a standard transaction, printing the appropriate merchant and cardholder receipts.

Upon completion, if the transaction is integrated, PAYware Ocius will return the integration response with additional fields added providing the Account on File payment details.

CARD WAIT

The Card Wait functionality has been introduced to provide additional integration flexibility for merchants.

The functionality allows for the integration to place PAYware Ocius in a wait state, prior to processing a transaction, ready for a card to be presented. The Card Wait functionality supports the following card capture methods; ICC, Keyed and Swipe transactions. Due to the nature of the functionality, it is not supported with Contactless transactions.

Once a card is presented and read by the terminal, the card details are returned to the POS and based upon this information a decision on how to continue to be made.

The card details presented are securely stored within the terminal and should the merchant decide to proceed with a transaction after receiving the response from the card wait record (CARDWAIT message type), then the card initially presented will not need to be re-inserted/swiped.

After the result from the card wait record has been returned to the POS, PAYware Ocius will remain in the card wait state and will need to be instructed to either:

- Card Wait state (CANCELCARDWAIT)
- Cancel Proceed with one of the following transaction types, utilising the store card details:
    - Barclays Gift transaction (BGIFT)
    - EFT transaction (T Record)
    - Park Retail Gift transaction (PRG)
    - PayPoint transaction (PPOINT)
    - SVS transaction (SVS)
- Request the last message be resent
- Screen position change (SCRPOS)
- Send a request for information command (REQINFO)
- Window state (WINSTATE)

Should a Cancel Card Wait request be sent to PAYware Ocius, all securely stored card details are removed from the terminal, before returning to the PAYware Ocius Main Menu.

Please note: *By default, the Card Wait response message will define the Capture Method as "ICC Unknown". This is due to the fact that the data is only being read from the card at this stage and no Cardholder Verification Method is required until a transaction is processed using the card.*

Card Wait Socket Disconnection

The following processes have been implemented in order for the solution to recover in the scenario whereby the socket connection to PAYware Ocius is disconnected unexpectedly:

- PAYware Ocius sends a CANCELCARDWAIT message to itself via the integration port upon start-up to ensure any previous card wait data status has been cleared
- When exiting PAYware Ocius, either via the close button on the graphical user interface or via logout command, PAYware Ocius sends itself a CANCELCARDWAIT command to clear any existing Card Wait status

These ensure that the merchant is not required to build the processes into the POS integration, as they are automatically handled.

Card Wait Request (CARDWAIT Record)

The request message should adhere to the following format:

FIELD	NAME	TYPE	DESCRIPTION
1	Message Identifier	String Mandatory	This is identifies the type of message. This will always be 'CARDWAIT'
2	Header	String Optional	This is the header text to display on the terminal when it prompts for the card details to be presented. To indicate that the section should be left empty, supply the following: <Blank> An empty field indicates that the terminal should display its standard data within this section
3	Body	String Optional	This is the body text to display on the terminal when it prompts for the card details to be presented. To indicate that the section should be left empty, supply the following: <Blank> An empty field indicates that the terminal should display its standard data within this section
4	Footer	String Optional	This is the footer text to display on the terminal when it prompts for the card details to be presented. To indicate that the section should be left empty, supply the following: <Blank> An empty field indicates that the terminal should display its standard data within this section
5	Wait for Card Timeout[7]	Integer	This is the time in seconds for the terminal to wait for the card

[7] PAYware Ocius will timeout 10 seconds after this timeout to try to ensure that the PED times out before PAYware Ocius does. This is similar to the wait for card timeout employed by standard transaction processing. In addition, the

		Optional	details to be presented. This value must be greater than or equal to 0 and must be less than or equal to the maximum value allowed for a 32-bit integer – 10 seconds when expressed in milliseconds (i.e. 2147483 seconds / 24 days). A value of 0 means do not timeout[8]. Default: 0
6	Allowed Capture Methods	String Optional	This is a hex bitmap of the capture methods that the terminal is to allow. The hex bitmap is comprised of the following hex values:- Keyed = 01 Swipe = 02 ICC = 04 Reserved = 08 Default: ICC + Swipe + Keyed = 07
7	Allowed Fallback Methods	String Optional	This is a hex bitmap of the fallback methods that the terminal is to allow. The hex bitmap is comprised of the following hex values:- Fallback from ICC to Swipe = 01 Fallback from Swipe to Key = 02 Default: Fallback from ICC to Swipe + Fallback from Swipe to Key = 03

Example record:

CARDWAIT,Welcome to The Shop,Please Present Card,Thank You,0,07,03

Card Wait Cancel Request (CANCELCARDWAIT Record)

In order to cancel a Card Wait request, the below message should be sent to PAYware Ocius:

FIELD	NAME	TYPE	DESCRIPTION
1	Message Identifier	String Mandatory	This is identifies the type of message. This will always be 'CANCELCARDWAIT'

The Card Wait Cancel request response will follow the same format as defined within the Card Wait Response.

The CANCELCARDWAIT command will be dependent on two scenarios; whether PAYware Ocius is still waiting for the card details or is in the "Wait for Card" transaction mode.

- If PAYware Ocius is still waiting for the card details, the Card Wait Cancel command must be sent down the existing socket connection (similar to the continue transaction commands). This is to allow other client connections to process a request.
- If PAYware Ocius is in the "Wait for Card" transaction mode, the original socket connection will no longer be available.

timeout is referenced against either the time that the request was sent to the PED or the last PED message received, whichever is the latter.

[8] PAYware Ocius will treat a value of zero for the wait for card timeout to be 2147463647 milliseconds (24 days)

Card Wait Response

The result of the card wait request will follow the below format:

FIELD	NAME	TYPE	DESCRIPTION
1	Result	Integer	This indicates the result of the Wait for Card request Valid values are:- Success = 0 Error = -ve The likely error codes are: -99 = Cancelled -135 = Wait for card timed out
2	Card Type	Integer	This indicates the type of card that was captured. Valid values are:- -1 = Not Recognised 0 = EFT 1 = Barclays Gift 2 = GiveX 3 = PayPoint 4 = SVS 5 = PayZone ETU 6 = Nectar 7 = Contis 8 = Ukash 9 = Park Retail (Flexecash) 10 = Merchant Specific Card Type 11 = Merchant Specific Card Type Default: Not Recognised = -1
3	Track2	String	This is the full track2 data of the non-EFT card.
4	PAN	String	For Standard EFT cards this will be the starred PAN using either the “all starred bar the first 6 and last 4” formatting or the “all starred bar the last 4” formatting as determined by configuration. For non-Standard EFT cards, which are identified as allowing the full PAN to be returned, this will be the full PAN. For non-EFT cards, this will be the full PAN.
5	Expiry Date / Application Expiration Date	String	This is the EFT card’s expiry date / application expiration date in the format MMYY, if applicable. For non-EFT cards, this field will not be returned.
6	Start Date / Application Effective Date	String	This is the EFT card’s start date / application effective date in the format MMYY, if applicable For non-EFT cards, this field will not be returned.
7	Issue Number / Application Sequence Number	String	This is the EFT card’s issue number / application sequence number, if applicable
8	Scheme Name	String	This is the scheme name as identified from the relevant IIN table entry used to identify the card
9	Capture Method	Integer	This identifies the method used to capture the card details. Valid values are:- Not Set = 0 Keyed Cardholder Present = 1 Keyed Cardholder Not Present (Mail Order) = 2 Swiped = 3 ICC Fallback To Swipe = 4 ICC Fallback To Signature = 5

			ICC PIN Only = 6 ICC PIN And Signature = 7 ICC No CVM = 8 *Contactless EMV = 9 *Contactless Magswipe = 10 Keyed Cardholder Not Present (Telephone Order) = 11 Keyed Cardholder Not Present (E-Commerce) = 12 ICC Unknown = 13 Keyed Cardholder Not Present (Account On File) = 14 * Contactless NOT supported (field reserved for future use)
10	Hash	String	This is a SHA-256 hash of the PAN with a merchant specific salt
11	Track1	String	This is the full track1 data of the non-EFT card.

VISA ADDITIONAL AUTHORISATION DATA (VAAD)

Visa has mandated that additional authorisation elements must be provided during domestic transactions in order to reduce the number of fraud transactions in the financial sector. The extra security information is intended to prevent fraud with all Visa debit and credit cards being used to pay off debts owed to merchants.

The changes will apply to merchants falling under the category of financial institutions which have Merchant Category Code 6012. These include; banks, payday loan lenders, securities brokers or dealers, insurance sales, insurance premiums and insurance carriers.

Please note: *All merchants within the MCC 6012 category will be required to ask for additional authorisation data when processing Visa transactions.*

Data Required

The additional authorisation data (AAD) will be required for transactions where cardholders use a Visa card to pay off outstanding debts. Examples of this type of transaction include paying off all, or part of, a balance on a credit card, payday loans, or mortgage repayments. The data will be required for all purchase payment types supported by Verifone.

The data will belong to the 'primary recipient'; the person whose debt is being paid-off, but who is not necessarily the cardholder. For example; if person 'A' owes debt to a loan lender and the debt is paid off by person 'B', then additional authorisation data for person 'A' will be required.

Merchants falling under the MCC 6012 category will be required to provide acquirers with the following additional authorisation data when processing transactions using Visa cards:

FIELD	INPUT	TYPE
Recipient date of birth	Year/Month/Day, e.g. 2014/12/01	String
Recipient surname	Up to 6 characters - if the surname is more than 6 characters long, then only the first 6 characters should be entered, e.g. for JOHNSON enter only JOHNSO	String
Recipient account number or partial PAN	Up to 10 alphanumeric characters of the account number (if the account number is less than 10 characters long, then the full account number should be provided). If entering a PAN – enter the first 6 and last 4 digits only, e.g. if PAN is 9999887766551234, then enter 9999881234	String
Recipient partial postcode	Up to 4 characters - The first part of the postcode (the district) e.g. if the postcode is TN24 8XW, enter only "TN24", or for the postcode B4 7DA only "B4" will be required.	String

Please note: *There are no case sensitive requirements for any of the VAAD fields.*

VAAD with Account on File (Tokenisation)

Currently, the solution does not support tokenisation with VAAD. The terminal will not prompt for AAD details when an Account on File transaction is performed. If a token transaction is processed via integration, then the VAAD details will be accepted however, the data will be removed prior to being passed to the acquirer for authorisation.

Terminal Input

To simplify the input of alphanumeric VAAD fields, a touchscreen QWERTY keyboard is available on the VX 680 Wi-Fi, Bluetooth and GPRS terminals, as well as the VX 820 Duet and VX 820 IP.

> ***Please note:*** *The terminal keypad is disabled when the touchscreen QWERTY keyboard is in use but the Enter and Cancel buttons will still be enabled.*

The VAAD prompts will appear after the card data is obtained and before cardholder verification, method functionality is used. Each prompt will timeout like a standard transaction after 30 seconds by default, this will cause that field to be skipped.

The images below illustrate how the VAAD prompts will appear on terminal screens:

> ***Please note:*** *The screenshots below are for illustrative purposes only.*

SHOW ORDER	REQUIRED FIELD	PROMPT SCREEN
1.	Date of birth	
2.	Surname	
3.	Account number or Partial PAN **Please note:** This prompt can be used to enter either the account number or the partial PAN. The terminal will NOT prompt separately for a partial PAN.	

4.	Postcode	

Please note: *The prompt screens will not permit the input of any symbols or special characters.*

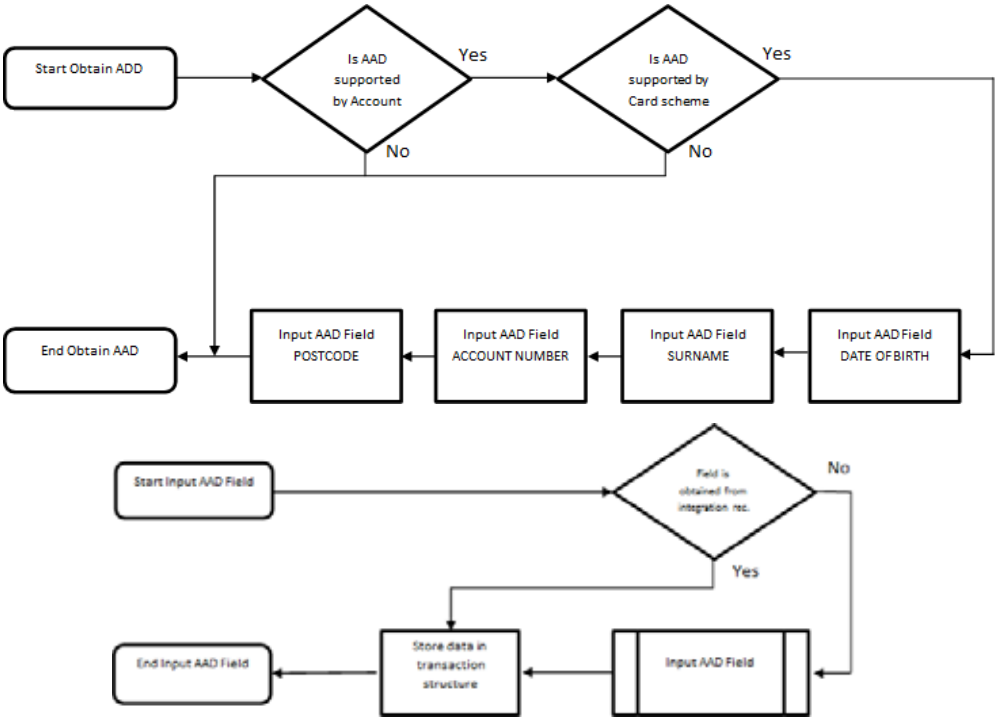
Data Storing

In the event when the terminal is offline, it will continue to prompt for the VAAD details. However, the data will not be stored as part of the OL Txn (Offline) information stored and it will be discarded.

Please note: *The additional authorisation data will not be logged at any point, even once encrypted.*

Obtain VAAD flow

The following image illustrates a high level process flow of how the VAAD details are obtained:



Integration Changes

It is possible to fill the required VAAD fields via integration. The fields are detailed in the table below:

T FIELD NUMBER	FIELD NAME	TYPE	VALIDATION
32	Date of birth	String	Length should be 8
33	Surname	String	-
34	Account number or Partial PAN	String	-
35	*Postcode	String	Length should be at least 2

Please note: **The postcode field allows up to 8 characters to be entered, but the terminal uses only the first half of the postcode which could be 2-4 characters in length for aadarec.*

The terminal will truncate fields to the maximum allowed size. If the integration record contains a VAAD field in which the length is exceeded, it will be truncated. For example, if the postcode length is exceeded, the field will be truncated to 8 characters and then truncated again to the first 4 characters of the postcode.

Please note: *Sending a field with an empty value is permitted, but in this case the empty field activates user screen prompt logic. It is possible to validate special characters, but this must be performed at the Point-of-Sale (POS). A field can also be skipped if the integration record contains a "_" symbol as the value ("_"). User input prompts will be shown automatically for the fields which have not been filled or skipped.*

Integration records pass the data in the clear and the terminals then encrypt and base 64 encode the data before sending onto the Verifone server.

Error Codes

The table below displays integration error response codes that may appear if invalid fields are entered:

CODE	TEXT	REASON
-186	INVALID DATE OF BIRTH	Length is not matched
-187	INVALID POSTCODE	Length is less than 2

Example of T record:

T,,01,0000,,,,,,,10.00,0.00,,,,,,,,,,ref,,,,,,,,,01022014,JHONSON,0123456789,LV1234

Example of T record with skipped surname field:

T,,01,0000,,,,,,,10.00,0.00,,,,,,,,,,ref,,,,,,,,,01022014,_,0123456789,LV1234

Please note: *The terminal will not validate the input of the Surname and Account number/PAN values, however validation will be performed by POS Client.*

VALUE-ADDED SERVICES

PAYware Ocius supports value-added services to ensure that a multi-channel payment solution is available to all merchants. value-added services provide merchants with the ability to offer their customers with additional services along with EFT transaction processing, such as loyalty schemes, pre-paid gift cards, gift vouchers, E-Top up etc.

Detailed within this section is an overview of all the value-added services supported with VX Evolution payment devices, and record formats utilised during integration.

Please note: *A value-added service is supported on only specific VX Evolution solutions due to acquirer certification requirements, for more details please contact your Sales Account Manager.*

BARCLAYCARD GIFT

Barclaycard Gift is a prepay gift card supported by Verifone's PAYware Ocius platform.

The gift card can be purchased in store from any participating merchant and has a prepaid balance, the amount of which is loaded upon purchase. The card can then be given as a gift to allow the cardholder to spend the balance at any of the participating merchants.

A 4 digit PIN is printed on the receipt when the gift card is initially purchased and can be used to access the balance of the card online at www.showmybalance.com.

Barclaycard Gift has 6 different transaction types available:

- Balance enquiry – return the remaining balance of the card
- New card/Top-Up – activate or top-up a gift card
- Sale – spend the value stored on the card in a participating merchant
- Refund – refund a value to the card from a previous transaction
- Cash – cash out a value from the gift card
- Void – void a previous transaction

As well as the standard gift transaction types, Barclaycard provide a cash function. This allows the gift cardholder to cash out the balance at a participating merchant.

Integration messages are provided to allow the POS to add Barclaycard Gift functionality, using the standard record format of a comma separated string followed by a carriage return line feed to be sent to the terminal. An acknowledgement will be generated by the terminal before the result is returned to the POS and the socket connection closed by PAYware Ocius.

Part payments are supported by the solution, enabling a purchase to be made using a combination of gift card funds and another form of payment.

In order to initiate a Barclaycard Gift transaction from the POS the below record should be constructed and sent in a comma separate format to PAYware Ocius.

Barclaycard Gift – Input Record

FIELD	NAME	TYPE	DESCRIPTION
1	Message Type	String *Mandatory*	This field will always be set to BGIFT.
2	Account ID	Decimal *Conditional*	This is the Account ID under which to process the transaction. Note: this is not required for void transactions, but is mandatory for all other transaction types.
3	Transaction Type	Integer *Mandatory*	The Barclaycard Gift transaction type: Balance Enquiry 1 New Card / Top-Up 2 Sale 3 Refund 4 Cash 5 Void 6
4	Amount	Decimal *Conditional*	This is the transaction value. Note: this is not required for Void/Balance Enquiry transaction types. For all other transaction types, this is mandatory.
5	Reference	Decimal *Conditional*	This is a merchant supplied reference used to track the transaction, e.g. within reporting. Note: the requirement of this field is defined within the Merchant configuration.
6	Original Transaction ID	Decimal *Conditional*	This is the Transaction ID of the original transaction to be voided. Note: this is mandatory for void transactions. For all other transaction types, this field should not be supplied.

Example Record:

BGIFT,,1,,Reference,

Barclaycard Gift – Output Record

FIELD	NAME	TYPE	DESCRIPTION
1	Result Code	Integer	This is the result of the transaction Valid values are: Success = 0 Reversed = 1 Rejected = 2 Error = -ve
2	Response Code	String	Ok = 0 NoCard = 10 CardValidButNotForThisMerchant = 20 PartialPurchaseTransaction = 30 ExchangeRateNotPresent = 40 MaximumLoadExceeded = 50 MinimumLoadNotMet = 51 MaximumValueOnCardExceeded = 52 CardExpired = 60 MessageTypeInvalid = 71 VoidPeriodElapsed = 72 MessageDetailsIncorrect = 73 InsufficientFunds = 74 CallCallCentre = 99 ConfigurationProblem = -1
3	Transaction Auth Code	String	This is the Auth Code given by Card Commerce
4	Amount	Decimal	This is the Amount of the Txn
5	Remaining Card Balance	Decimal	This is the remaining Balance of the card returned in the transaction response
6	Message	String	This is the Authorisation message indicating the success of the transaction
7	Message Number	String	
8	Transaction Date/Time	String	This is in the format dd MMM yyyy HH:mm:ss
9	Verifone Transaction ID	Decimal	This is the Transaction ID assigned by Verifone's processing system

Example Output Record:

0,00,003739131,0.00,79.14,Expiry:03/04/2010,2076, 29/12/2009 11:00:17 ,3164

DYNAMIC CURRENCY CONVERSION (DCC)

As companies become increasingly globalised and cheaper travel encourages individuals to travel the world more and more frequently, the need for retailers to increase footfall from international tourists has become more pressing. Dynamic Currency Conversion (DCC), provided by FEXCO, offers retailers the functionality to allow overseas customers to make purchases by Visa and MasterCard in their home billing currency.

On entering the customer's credit card into Verifone's PAYware Ocius card payment solution, DCC will identify a payment card's country of origin and offers the customer the option of paying in their home currency. DCC will look up the exchange rates for that day's trading and calculate the price in the requested currency to enable the buyer to select their transaction currency of choice.

When processing a DCC transaction, prior to authorisation, the cardholder is asked to confirm that they are happy with the rate of exchange being offered and are given the option to pay in the original currency or the transaction currency.

A receipt is produced at this stage, as well as on-screen prompts being displayed for the cardholder to respond to (to select which currency is desired).

The exchange rate is guaranteed, ensuring that the merchant will always receive payment in their home currency, a percentage of the foreign exchange difference from the Acquirer and removes any exchange rate risk.

E-TOP-UP (MOBILE TOP-UP)

The past few years have seen rapid growth in prepay mobile phone customers choosing to "Top-up" electronically. This has opened a new market for retailers who are able to earn a commission on a product that avoids any of the normal problems associated with stocking and distributing a physical item.

The functionality is supported on certain VX Evolution solutions offering retailers E-Top-ups easily and cost effectively at the point of sale. The solutions provide a combined E-Top-up and card processing solution that can be integrated with existing POS systems. Verifone's E-Top-up solution works with all the leading mobile networks (for details on supported solutions, please contact your Sales Account Manager).

ETU provides merchants with the ability to process mobile phone top up transactions for customers using their E-Top-up card, to link to their pre-pay mobile phone account. If payment needs to be collected via card before the E-Top-up then this can be performed by PAYware Ocius, and the Merchant can then process the top up after confirming the money was debited from the cardholders account.

There is only a customer receipt required for this process and as such, no merchant receipts are produced.

E-Top-up – Input Record

Integrated E-Top-up Transactions are triggered by supplying an E Record via text file to the monitored directory, or via a direct socket connection to PAYware Ocius.

It is possible to send a record of 'E,,,,,,,' to trigger a manual E-Top-up; whereby the data is requested at each step of the transaction process (Card Number, Amount...).

When supplied, the Card Number and Capture Method fields within the record are conditional upon each other; one cannot be passed without the other.

To pass an Integrated Record containing the E-Voucher Product Code, the Capture Method field should be set to '1' for manual, and the code placed in the 7th field. The code will need to be taken from the 'ETUEVoucherIIN.txt' file. This file contains the E-Voucher product list, and the Product Code required is the second field. An example product listing taken from the file, with the value to be referenced shown in bold:

10;**9894410000**;1;Vodafone EVoucher;5|10|15|20|25|30|40|50;Pound Sterling;GBP;#;.;;2;826

When passed, the record should be followed with a carriage return/line feed pair. This will initialise an E-Top-up transaction:

FIELD	NAME	TYPE	DESCRIPTION
1	Record Type	String	'E' – Indicates an E-Top-up record.
2	ETU Account ID	Decimal	The ETU Account ID as allocated by Verifone
3	ETU Type	Integer	'1' – E-Top-up '2' – E-Voucher
4	Transaction Type	Integer	'04' – Sale
5	Transaction Amount	Decimal	Value of the transaction, e.g. 10.00
6	Capture Method	Integer Conditional	'0' – Swiped '1' – Manual
7	Card Number/Product ID	Decimal Conditional	If capture method is swiped this should be the full track2 data, including start and end sentinels and LRC. If manual, either the card number or the Product ID (from 'ETUEVoucherIIN.txt') is required.
8	Original Transaction Identifier	Decimal	Reserved for future use

Please note: E-Top-Up refunds are not supported by the service provider or the network operators.

E-Top-up – Output Record

Once the E-Top-Up has been completed, a response record is returned to the POS:

FIELD	NAME	TYPE	DESCRIPTION
1	Msg Type	String	'R' – Indicates a response record
2	Result	String	'0' – Successful '7' – Failed '-nn' – Error
3	Transaction Identifier	String	Authorisation code from mobile phone host
4	ETU Account ID	Decimal	Merchant ETU Account ID ref. ETUAccounts.txt
5	ETU Type	Integer	'1' – E-Top Up '2' – E-Voucher
6	Transaction Type	Integer	'04' – Sale '07' – Void
7	ETU Product ID	Decimal	Product from ETUEVoucherIIN.Txt or ETUECardIIN.txt
8	ETU Operator ID	Decimal	Ref. ETUOperators.txt
9	Transaction Amount	Decimal	Monetary value of Top Up e.g. 10.00
10	Card Number	Decimal	Card number from Top Up card
11	Transaction Date Time	Decimal	Transaction date and time, In the format dd-mm-yyyy hh:mm:ss
12	Response Message	String	Describes transaction outcome

SVS

Stored Value Solutions provide prepaid services to merchants. Verifone support SVS' branded prepaid cards which are used to:

- Reward and incentivise employees, customers, and partners
- Improve foot traffic to your locations
- Increase brand awareness
- Facilitate new promotional and co-branding opportunities
- Allow easy gift card acceptance across multiple point-of-sale systems

Prepaid cards are accepted the same way as any standard electronic funds transfer card through Verifone's PAYware Ocius platform. The transaction types are listed in full within the integration records; with support for Balance Enquiry, Redemption, Card Reload and Cash out included.

Reconciliation is automated via a daily settlement file sent to SVS from the Verifone host.

The option to use SVS' Interactive Voice Recognition (IVR) System is also provided should this be required.

Please note: *The merchant must have an agreement and account setup with SVS in order to allow Verifone to enable the functionality on the terminal. For more details, please speak to your Sales Account Manager.*

To support integrated Stored Value Solution transactions a comma delimited integration record must be supplied, conforming to the below format:

SVS – Input Record

FIELD	NAME	TYPE	LENGTH (MAX)	DESCRIPTION
1	Message Type	String	3	This field will always be set to SVS.
2	Transaction Type	Integer	3	Valid values are: Balance Enquiry 0 *Pre-Authorization 1 Redemption 2 *Tip 3 Cancellation 4 Return 5 Card Reload 6 *Pre-Auth Completion 7 *Activate Card 8 Issue Card 9 *Issue Virtual Card 10 *Network Message 12 Cash Out 13 [* = reserved for future use] **Please note:** reversals are not supported via integration as they are catered for automatically by the Managed Service
3	Amount	Decimal	8	The amount of the SVS transaction
4	Account ID	String	12	The Account under which the transaction is to be processed
5	STAN	String	6	Systems Trace Audit Number

Example record:

SVS,9,1.00,10459,123456

SVS – Output Record

Upon completion of the SVS transaction, the terminal will provide the POS with a comma delimited message in the below format:

FIELD	NAME	TYPE	LENGTH (MAX)	DESCRIPTION
1	Response Code	String	3	SVS response codes: None 0 Approved 1 Card Inactive 2 Invalid Card Number 3 Invalid Transaction Code 4 Insufficient Funds 5 No Previous Transaction 6 Invalid Message 7 No Card Found 8 Insufficient Funds Pre-Auth 9 Denial No Previous Auth 10 Exceeded Maximum Single Reloads 13 Exceeded Max Balance 14 Shut Down 15 Invalid Card Status 16

				Unknown Store Number Exceeded Max Reloads Invalid Verification Value Invalid Pin Number Card Already Issued Card Not Issued Card Already Used Manual Transaction Not Allowed Invalid Magnetic Read Unknown Transaction Type Invalid Tender Type Invalid Customer Type Pin Locked Exceeded Maximum Redemptions Invalid Currency Code Invalid Server ID Frozen Invalid Amount Application Error Cancelled	17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 -1 -99
2	Amount	String	8	Value of the transaction	
3	Balance	String	8	Value of the card balance	
4	Currency Code	String	4	Standard accepted alpha code of the currency (e.g. GBP)	
5	Conversion Rate	String	8	Conversion rate between merchant and cardholder currencies	
6	Masked PAN	String	20	Masked Card number used in the transaction	
7	STAN	String	6	Systems Trace Audit Number	
8	Message	String	Variable	Text returned by SVS host server	

Example record:

01,0.00,39.99,GBP,1.00000,**********4179,110009,Approval

MOBILE VOUCHERS

Mobile Vouchers, provided by Eagle Eye Solutions, provide retailers with the full story from initial purchase to in-store redemption and beyond. The mobile gift voucher technology enables merchants with the ability to remain engaged with their customers.

Mobile Vouchers eliminate the need for plastic or paper gift vouchers, saving on printing, and postage and transport costs proving to be cost effective for businesses.

As the voucher is issued via mobile, a reminder message is sent to the recipient, making un-redeemed gift vouchers a thing of the past. When the code is entered into the EPOS, the system instantly acknowledges that unique one-off code has now been used, and generates a CRM report (containing details of the transaction). If the customer uses only part of the balance and has remaining fund left on the voucher, then the system will send a new mobile gift voucher to the customer for the exact amount remaining to be redeemed another time.

CONTIS

Contis gift cards are used by retailers to increase brand awareness, loyalty and to encourage customer footfall in store and to boost sales online. Contis provide businesses with choice and flexibility, to ensure an individual retailer's gift card scheme suits the needs of its business strategy and objectives.

Other benefits of Contis gift cards for retailer include: a reduction in overhead costs, management reporting, front of wallet visibility and an interactive marketing tool. Customers also find them easy and convenient to use and find them ideal as a last minute gift.

PENNIES

Pennies is a charitable donation, created by the Pennies Foundation. It is an electronic charity box which is designed to make giving to charity easy, quick and affordable. It's new, inclusive and will raise additional money for many UK registered charities.

With one touch of a button shoppers can choose to donate a few pennies in private when they pay by debit card, credit card or electronically.

Types of Pennies donation supported:

- Top Up - ability to top up transaction amount by a pre-defined amount
- Round Up - ability to round up the transaction value to the nearest amount

Configuration

Merchants can configure the functionality to either round up to the nearest adjustment value (e.g. the nearest £1) or top up according to the adjustment value (e.g. top up by £1). For example, if the total payment due is £9.50 then the charitable donation could be configured to round up to £10.00, or top up by 50p to make the total value as £10.00.

All the pennies are then added together and all of the money that's been collected is given to UK charities, both big and small.

Please note: *The adjustment value is configured on the merchant account. Please contact Verifone Merchant Helpdesk for any queries.*

Although merchants are required to have a Pennies MID setup; there is no requirement for the merchant to notify their acquiring bank of their participation in the service, as the Pennies amounts are incorporated into the EFT transaction value sent to the bank for authorisation and settlement.

Pennies will invoice each merchant at the end of the month for the amount of donations made via their Pennies MID. The settlement amounts are then settled between the merchant and Pennies directly. Should the merchant have any discrepancies with the amounts invoiced they should look to contact Pennies directly.

Screen Prompt

The Pennies prompt will be displayed on the terminal screen once the total price has been calculated, and the cardholder is ready to pay for the goods. The cardholder will be prompted whether they wish to donate and the value will be displayed on the screen, depending on the configuration of a round up or top up.

The cardholder will be able to select 'Yes' or 'No', indicated by options on the screen and the keypad. If the cardholder elects to donate, then the total value will be recalculated and the transaction can be completed.

Please note: *The Pennies and Contis Value-adds are currently only supported on stand-alone terminals and are not supported by integration.*

Pennies Supported Solutions

The table below details the Verifone platforms that currently support Pennies and their accreditation status:

SOLUTION	SUPPORTED	SOFTWARE VERSION	PENNIES ACCREDITATION STATUS
PAYware Ocius POS Client with V^{X}810	**P**	POS Client - v03.05.02.12 V^{X}810 - v03.05.08.18486	**P**
PAYware Ocius POS Client with VX820	**P**	POS Client- v03.56.02.07 VX820 - v03.07.24.18877	**P**
PAYware Ocius VX680 GPRS	**P**	v03.50.00.10	**P**
PAYware Ocius VX680 Bluetooth	**P**	v03.50.00.10	**P**

APPENDIX

CURRENCY CODE ISO 4217

CURRENCY	CODE	NUM	LOCATIONS USING THIS CURRENCY
Afghani	AFN	971	Afghanistan
Algerian dinar	DZD	012	Algeria
Argentine peso	ARS	032	Argentina
Armenian dram	AMD	051	Armenia
Aruban guilder	AWG	533	Aruba
Australian dollar	AUD	036	Australia, Australian Antarctic Territory, Christmas Island, Cocos (Keeling) Islands, Heard and McDonald Islands, Kiribati, Nauru, Norfolk Island, Tuvalu
Azerbaijanian manat	AZN	944	Azerbaijan
Bahamian dollar	BSD	044	Bahamas
Bahraini dinar	BHD	048	Bahrain
Baht	THB	764	Thailand
Balboa	PAB	590	Panama
Bangladeshi taka	BDT	050	Bangladesh
Barbados dollar	BBD	052	Barbados
Belarusian ruble	BYR	974	Belarus
Belize dollar	BZD	084	Belize
Bermudian dollar (customarily known as Bermuda dollar)	BMD	060	Bermuda
Bolivian Mvdol (funds code)	BOV	984	Bolivia
Boliviano	BOB	068	Bolivia
Brazilian real	BRL	986	Brazil
Brunei dollar	BND	096	Brunei, Singapore
Bulgarian lev	BGN	975	Bulgaria
Burundian franc	BIF	108	Burundi
Canadian dollar	CAD	124	Canada
Cape Verde escudo	CVE	132	Cape Verde
Cayman Islands dollar	KYD	136	Cayman Islands
Cedi	GHS	936	Ghana
CFA Franc BCEAO	XOF	952	Benin, Burkina Faso, Côte d'Ivoire, Guinea-Bissau, Mali, Niger, Senegal, Togo
CFA franc BEAC	XAF	950	Cameroon, Central African Republic, Congo, Chad, Equatorial Guinea, Gabon
CFP franc	XPF	953	French Polynesia, New Caledonia, Wallis and Futuna
Chilean peso	CLP	152	Chile
Chinese Yuan	CNY	156	China (Mainland)
Code reserved for testing purposes	XTS	963	
Colombian peso	COP	170	Colombia
Comoro franc	KMF	174	Comoros
Convertible marks	BAM	977	Bosnia and Herzegovina
Cordoba oro	NIO	558	Nicaragua
Costa Rican colon	CRC	188	Costa Rica
Croatian kuna	HRK	191	Croatia
Cuban convertible peso	CUC	931	Cuba
Cuban peso	CUP	192	Cuba
Czech Koruna	CZK	203	Czech Republic
Dalasi	GMD	270	Gambia
Danish krone	DKK	208	Denmark, Faroe Islands, Greenland
Denar	MKD	807	Macedonia
Djibouti franc	DJF	262	Djibouti
Dobra	STD	678	São Tomé and Príncipe
Dominican peso	DOP	214	Dominican Republic

East Caribbean dollar	XCD	951	Anguilla, Antigua and Barbuda, Dominica, Grenada, Montserrat, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines
Egyptian pound	EGP	818	Egypt
Ethiopian birr	ETB	230	Ethiopia
Euro	EUR	978	Austria, Belgium, Cyprus, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Malta, Netherlands, Portugal, Slovakia, Slovenia, Spain, Andorra, Kosovo, Monaco, Montenegro, San Marino, Vatican
European Composite Unit (EURCO) (bond market unit)	XBA	955	
European Monetary Unit (E.M.U.-6) (bond market unit)	XBB	956	
European Unit of Account 17 (E.U.A.-17) (bond market unit)	XBD	958	
European Unit of Account 9 (E.U.A.-9) (bond market unit)	XBC	957	
Falkland Islands pound	FKP	238	Falkland Islands
Fiji dollar	FJD	242	Fiji
Forint	HUF	348	Hungary
Franc Congolais	CDF	976	Democratic Republic of Congo
Gibraltar pound	GIP	292	Gibraltar
Gold (one troy ounce)	XAU	959	
Guarani	PYG	600	Paraguay
Guinea franc	GNF	324	Guinea
Guyana dollar	GYD	328	Guyana
Haiti gourde	HTG	332	Haiti
Hong Kong dollar	HKD	344	Hong Kong Special Administrative Region
Hryvnia	UAH	980	Ukraine
Iceland krona	ISK	352	Iceland
Indian rupee	INR	356	Bhutan, India
Iranian rial	IRR	364	Iran
Iraqi dinar	IQD	368	Iraq
Israeli new sheqel	ILS	376	Israel
Jamaican dollar	JMD	388	Jamaica
Japanese yen	JPY	392	Japan
Jordanian dinar	JOD	400	Jordan
Kenyan shilling	KES	404	Kenya
Kina	PGK	598	Papua New Guinea
Kip	LAK	418	Laos
Kroon	EEK	233	Estonia
Kuwaiti dinar	KWD	414	Kuwait
Kwacha	MWK	454	Malawi
Kwacha	ZMK	894	Zambia
Kwanza	AOA	973	Angola
Kyat	MMK	104	Myanmar
Lari	GEL	981	Georgia
Latvian lats	LVL	428	Latvia
Lebanese pound	LBP	422	Lebanon
Lek	ALL	008	Albania
Lempira	HNL	340	Honduras
Leone	SLL	694	Sierra Leone
Lesotho loti	LSL	426	Lesotho
Liberian dollar	LRD	430	Liberia
Libyan dinar	LYD	434	Libya
Lilangeni	SZL	748	Swaziland
Lithuanian litas	LTL	440	Lithuania
Malagasy ariary	MGA	969	Madagascar
Malaysian ringgit	MYR	458	Malaysia
Manat	TMT	934	Turkmenistan
Mauritius rupee	MUR	480	Mauritius
Metical	MZN	943	Mozambique

Mexican peso	MXN	484	Mexico
Mexican Unidad de Inversion (UDI) (funds code)	MXV	979	Mexico
Moldovan leu	MDL	498	Moldova
Moroccan dirham	MAD	504	Morocco, Western Sahara
Naira	NGN	566	Nigeria
Nakfa	ERN	232	Eritrea
Namibian dollar	NAD	516	Namibia
Nepalese rupee	NPR	524	Nepal
Netherlands Antillean guilder	ANG	532	Netherlands Antilles
New Taiwan dollar	TWD	901	Taiwan and other islands that are under the effective control of the Republic of China (ROC)
New Zealand dollar	NZD	554	Cook Islands, New Zealand, Niue, Pitcairn, Tokelau
Ngultrum	BTN	064	Bhutan
No currency	XXX	999	
North Korean won	KPW	408	North Korea
Norwegian krone	NOK	578	Norway, Bouvet Island, Queen Maud Land, Peter I Island
Nuevo sol	PEN	604	Peru
Ouguiya	MRO	478	Mauritania
Pa'anga	TOP	776	Tonga
Pakistan rupee	PKR	586	Pakistan
Palladium (one troy ounce)	XPD	964	
Pataca	MOP	446	Macau Special Administrative Region
Peso Uruguayo	UYU	858	Uruguay
Philippine peso	PHP	608	Philippines
Platinum (one troy ounce)	XPT	962	
Pound sterling	GBP	826	United Kingdom, Crown Dependencies (the Isle of Man and the Channel Islands), certain British Overseas Territories (South Georgia and the South Sandwich Islands, British Antarctic Territory and British Indian Ocean Territory)
Pula	BWP	072	Botswana
Qatari rial	QAR	634	Qatar
Quetzal	GTQ	320	Guatemala
Rial Omani	OMR	512	Oman
Riel	KHR	116	Cambodia
Romanian new leu	RON	946	Romania
Rufiyaa	MVR	462	Maldives
Rupiah	IDR	360	Indonesia
Russian rouble	RUB	643	Russia, Abkhazia, South Ossetia
Rwanda franc	RWF	646	Rwanda
Saint Helena pound	SHP	654	Saint Helena
Samoan tala	WST	882	Samoa
Saudi riyal	SAR	682	Saudi Arabia
Serbian dinar	RSD	941	Serbia
Seychelles rupee	SCR	690	Seychelles
Silver (one troy ounce)	XAG	961	
Singapore dollar	SGD	702	Singapore, Brunei
Solomon Islands dollar	SBD	090	Solomon Islands
Som	KGS	417	Kyrgyzstan
Somali shilling	SOS	706	Somalia
Somoni	TJS	972	Tajikistan
South African rand	ZAR	710	South Africa
South Korean won	KRW	410	South Korea
Special Drawing Rights	XDR	960	International Monetary Fund
Sri Lanka rupee	LKR	144	Sri Lanka
Sudanese pound	SDG	938	Sudan
Surinam dollar	SRD	968	Suriname
Swedish krona/kronor	SEK	752	Sweden
Swiss franc	CHF	756	Switzerland, Liechtenstein
Syrian pound	SYP	760	Syria
Tanzanian shilling	TZS	834	Tanzania

Tenge	KZT	398	Kazakhstan
Trinidad and Tobago dollar	TTD	780	Trinidad and Tobago
Tugrik	MNT	496	Mongolia
Tunisian dinar	TND	788	Tunisia
Turkish lira	TRY	949	Turkey, Northern Cyprus
Uganda shilling	UGX	800	Uganda
UIC franc (special settlement currency)	XFU	Nil	International Union of Railways
Unidad de Fomento (funds code)	CLF	990	Chile
Unidad de Valor Real	COU	970	Colombia
United Arab Emirates dirham	AED	784	United Arab Emirates
United States dollar (next day) (funds code)	USN	997	United States
United States dollar (same day) (funds code) (one source[*who?*] claims it is no longer used, but it is still on the ISO 4217-MA list)	USS	998	United States
US dollar	USD	840	American Samoa, British Indian Ocean Territory, Ecuador, El Salvador, Guam, Haiti, Marshall Islands, Micronesia, Northern Mariana Islands, Palau, Panama, Puerto Rico, Timor-Leste, Turks and Caicos Islands, United States, Virgin Islands, Bermuda (as well as Bermudian Dollar)
Uzbekistan som	UZS	860	Uzbekistan
Vatu	VUV	548	Vanuatu
Venezuelan bolívar fuerte	VEF	937	Venezuela
Vietnamese đồng	VND	704	Vietnam
WIR euro (complementary currency)	CHE	947	Switzerland
WIR franc (complementary currency)	CHW	948	Switzerland
Yemeni rial	YER	886	Yemen
Zimbabwe dollar	ZWL	932	Zimbabwe
Złoty	PLN	985	Poland

COUNTRY CODES ISO 3166

OFFICIAL COUNTRY NAMES USED BY THE ISO 3166/MA	NUMERIC	ALPHA-3	ALPHA-2
Afghanistan	004	AFG	AF
Åland Islands	248	ALA	AX
Albania	008	ALB	AL
Algeria	012	DZA	DZ
American Samoa	016	ASM	AS
Andorra	020	AND	AD
Angola	024	AGO	AO
Anguilla	660	AIA	AI
Antarctica	010	ATA	AQ
Antigua and Barbuda	028	ATG	AG
Argentina	032	ARG	AR
Armenia	051	ARM	AM
Aruba	533	ABW	AW
Australia	036	AUS	AU
Austria	040	AUT	AT
Azerbaijan	031	AZE	AZ
Bahamas	044	BHS	BS
Bahrain	048	BHR	BH
Bangladesh	050	BGD	BD
Barbados	052	BRB	BB
Belarus	112	BLR	BY
Belgium	056	BEL	BE
Belize	084	BLZ	BZ
Benin	204	BEN	BJ
Bermuda	060	BMU	BM
Bhutan	064	BTN	BT
Bolivia	068	BOL	BO
Bosnia and Herzegovina	070	BIH	BA
Botswana	072	BWA	BW
Bouvet Island	074	BVT	BV
Brazil	076	BRA	BR
British Indian Ocean Territory	086	IOT	IO
Brunei Darussalam	096	BRN	BN
Bulgaria	100	BGR	BG
Burkina Faso	854	BFA	BF
Burundi	108	BDI	BI
Cambodia	116	KHM	KH
Cameroon	120	CMR	CM
Canada	124	CAN	CA
Cape Verde	132	CPV	CV
Cayman Islands	136	CYM	KY
Central African Republic	140	CAF	CF
Chad	148	TCD	TD
Chile	152	CHL	CL
China	156	CHN	CN
Christmas Island	162	CXR	CX
Cocos (Keeling) Islands	166	CCK	CC
Colombia	170	COL	CO
Comoros	174	COM	KM
Congo	178	COG	CG
Congo, Democratic Republic of the	180	COD	CD
Cook Islands	184	COK	CK
Costa Rica	188	CRI	CR
Côte d'Ivoire	384	CIV	CI
Croatia	191	HRV	HR
Cuba	192	CUB	CU
Cyprus	196	CYP	CY

Czech Republic	203	CZE	CZ
Denmark	208	DNK	DK
Djibouti	262	DJI	DJ
Dominica	212	DMA	DM
Dominican Republic	214	DOM	DO
Ecuador	218	ECU	EC
Egypt	818	EGY	EG
El Salvador	222	SLV	SV
Equatorial Guinea	226	GNQ	GQ
Eritrea	232	ERI	ER
Estonia	233	EST	EE
Ethiopia	231	ETH	ET
Falkland Islands (Malvinas)	238	FLK	FK
Faroe Islands	234	FRO	FO
Fiji	242	FJI	FJ
Finland	246	FIN	FI
France	250	FRA	FR
French Guiana	254	GUF	GF
French Polynesia	258	PYF	PF
French Southern Territories	260	ATF	TF
Gabon	266	GAB	GA
Gambia	270	GMB	GM
Georgia	268	GEO	GE
Germany	276	DEU	DE
Ghana	288	GHA	GH
Gibraltar	292	GIB	GI
Greece	300	GRC	GR
Greenland	304	GRL	GL
Grenada	308	GRD	GD
Guadeloupe	312	GLP	GP
Guam	316	GUM	GU
Guatemala	320	GTM	GT
Guernsey	831	GGY	GG
Guinea	324	GIN	GN
Guinea-Bissau	624	GNB	GW
Guyana	328	GUY	GY
Haiti	332	HTI	HT
Heard Island and McDonald Islands	334	HMD	HM
Holy See (Vatican City State)	336	VAT	VA
Honduras	340	HND	HN
Hong Kong	344	HKG	HK
Hungary	348	HUN	HU
Iceland	352	ISL	IS
India	356	IND	IN
Indonesia	360	IDN	ID
Iran, Islamic Republic of	364	IRN	IR
Iraq	368	IRQ	IQ
Ireland	372	IRL	IE
Isle of Man	833	IMN	IM
Israel	376	ISR	IL
Italy	380	ITA	IT
Jamaica	388	JAM	JM
Japan	392	JPN	JP
Jersey	832	JEY	JE
Jordan	400	JOR	JO
Kazakhstan	398	KAZ	KZ
Kenya	404	KEN	KE
Kiribati	296	KIR	KI
Korea, Democratic People's Republic of	408	PRK	KP
Korea, Republic of	410	KOR	KR
Kuwait	414	KWT	KW

Kyrgyzstan	417	KGZ	KG
Lao People's Democratic Republic	418	LAO	LA
Latvia	428	LVA	LV
Lebanon	422	LBN	LB
Lesotho	426	LSO	LS
Liberia	430	LBR	LR
Libyan Arab Jamahiriya	434	LBY	LY
Liechtenstein	438	LIE	LI
Lithuania	440	LTU	LT
Luxembourg	442	LUX	LU
Macao	446	MAC	MO
Macedonia, the former Yugoslav Republic of	807	MKD	MK
Madagascar	450	MDG	MG
Malawi	454	MWI	MW
Malaysia	458	MYS	MY
Maldives	462	MDV	MV
Mali	466	MLI	ML
Malta	470	MLT	MT
Marshall Islands	584	MHL	MH
Martinique	474	MTQ	MQ
Mauritania	478	MRT	MR
Mauritius	480	MUS	MU
Mayotte	175	MYT	YT
Mexico	484	MEX	MX
Micronesia, Federated States of	583	FSM	FM
Moldova, Republic of	498	MDA	MD
Monaco	492	MCO	MC
Mongolia	496	MNG	MN
Montenegro	499	MNE	ME
Montserrat	500	MSR	MS
Morocco	504	MAR	MA
Mozambique	508	MOZ	MZ
Myanmar	104	MMR	MM
Namibia	516	NAM	NA
Nauru	520	NRU	NR
Nepal	524	NPL	NP
Netherlands	528	NLD	NL
Netherlands Antilles	530	ANT	AN
New Caledonia	540	NCL	NC
New Zealand	554	NZL	NZ
Nicaragua	558	NIC	NI
Niger	562	NER	NE
Nigeria	566	NGA	NG
Niue	570	NIU	NU
Norfolk Island	574	NFK	NF
Northern Mariana Islands	580	MNP	MP
Norway	578	NOR	NO
Oman	512	OMN	OM
Pakistan	586	PAK	PK
Palau	585	PLW	PW
Palestinian Territory, Occupied	275	PSE	PS
Panama	591	PAN	PA
Papua New Guinea	598	PNG	PG
Paraguay	600	PRY	PY
Peru	604	PER	PE
Philippines	608	PHL	PH
Pitcairn	612	PCN	PN
Poland	616	POL	PL
Portugal	620	PRT	PT
Puerto Rico	630	PRI	PR
Qatar	634	QAT	QA

Réunion	638	REU	RE
Romania	642	ROU	RO
Russian Federation	643	RUS	RU
Rwanda	646	RWA	RW
Saint Helena	654	SHN	SH
Saint Kitts and Nevis	659	KNA	KN
Saint Lucia	662	LCA	LC
Saint Pierre and Miquelon	666	SPM	PM
Saint Vincent and the Grenadines	670	VCT	VC
Samoa	882	WSM	WS
San Marino	674	SMR	SM
São Tomé and Príncipe	678	STP	ST
Saudi Arabia	682	SAU	SA
Senegal	686	SEN	SN
Serbia	688	SRB	RS
Seychelles	690	SYC	SC
Sierra Leone	694	SLE	SL
Singapore	702	SGP	SG
Slovakia	703	SVK	SK
Slovenia	705	SVN	SI
Solomon Islands	090	SLB	SB
Somalia	706	SOM	SO
South Africa	710	ZAF	ZA
South Georgia and the South Sandwich Islands	239	SGS	GS
Spain	724	ESP	ES
Sri Lanka	144	LKA	LK
Sudan	736	SDN	SD
Suriname	740	SUR	SR
Svalbard and Jan Mayen	744	SJM	SJ
Swaziland	748	SWZ	SZ
Sweden	752	SWE	SE
Switzerland	756	CHE	CH
Syrian Arab Republic	760	SYR	SY
Taiwan, Province of China	158	TWN	TW
Tajikistan	762	TJK	TJ
Tanzania, United Republic of	834	TZA	TZ
Thailand	764	THA	TH
Timor-Leste	626	TLS	TL
Togo	768	TGO	TG
Tokelau	772	TKL	TK
Tonga	776	TON	TO
Trinidad and Tobago	780	TTO	TT
Tunisia	788	TUN	TN
Turkey	792	TUR	TR
Turkmenistan	795	TKM	TM
Turks and Caicos Islands	796	TCA	TC
Tuvalu	798	TUV	TV
Uganda	800	UGA	UG
Ukraine	804	UKR	UA
United Arab Emirates	784	ARE	AE
United Kingdom	826	GBR	GB
United States	840	USA	US
United States Minor Outlying Islands	581	UMI	UM
Uruguay	858	URY	UY
Uzbekistan	860	UZB	UZ
Vanuatu	548	VUT	VU
Venezuela	862	VEN	VE
Viet Nam	704	VNM	VN
Virgin Islands, British	092	VGB	VG
Virgin Islands, U.S.	850	VIR	VI
Wallis and Futuna	876	WLF	WF

Western Sahara	732	ESH	EH
Yemen	887	YEM	YE
Zambia	894	ZMB	ZM
Zimbabwe	716	ZWE	ZW

VERIFONE ERROR CODES

The following table illustrates a generic list of PAYware Ocius error codes, with descriptions and recommended actions required.

Please note: *Depending on the method of integration and communication means utilised, not all the error codes listed will be applicable.*

ERROR CODE	GENERAL DESCRIPTION	ADDITIONAL TECHNICAL DESCRIPTION (IF REQUIRED)	RECOMMENDED ACTION
-1	Unspecified error		Contact Verifone
-2	Invalid transaction type	An example of this could be a Refund being passed when the site are not set up to do so. A trace of what was passed will be in the system log.	Use alternative method for transaction type.
-3	Invalid card / invalid Track2	General card error. Track2 must either be ;PAN=YYMMsss……?x or just the PAN.	Re-enter card number or re-swipe card
-4	Card scheme not recognised	The card Issuer Identification Number (IIN) has not been located in the IIN table. The IIN is typically the first 4 to 6 digits of the card number.	Prompt for alternate method of payment
-5	Card scheme not accepted	The card has been identified, but the card scheme is not accepted at the given site.	Reject Transaction
-6	Invalid card number (lcd)	The LUHN check digit is incorrect (the card has been mis-keyed or mis-swiped).	Re-enter card number or re-swipe card
-7	Invalid card number length	The length of the PAN is incorrect for the given card scheme.	Re-enter card number or re-swipe card
-8	Invalid card number (pcd)	The pen-ultimate check digit is invalid.	Re-enter card number or re-swipe card
-9	Expired card		Prompt for alternate method of payment
-10	Card not yet valid		Prompt for alternate method of payment
-11	Invalid card service code	The Track2 service code is invalid.	Prompt for alternate method of payment
-12	File or XML missing or wrong format	A required file or XML is missing or has wrong format.	Contact Verifone
-13	File permanently locked	A file required by the EFT library was still locked after EFT FIO TRIES attempts.	Contact Verifone
-14	Out of memory	The library has failed to allocate sufficient heap.	Contact Verifone
-15	Account number does not exist	The requested account number does not exist.	Check the account number configuration of the system, ensuring it matches that configured within WinTI
-16	Value exceeds ceiling limit	Purchase value exceeds card scheme ceiling limit	Prompt for alternative method of payment. Arrange to increase ceiling limits

-17	Cashback exceeds ceiling limit	Cashback value exceeds card scheme ceiling limit	Revise transaction cash-back value
-18	Transaction currency is invalid	The transaction currency code is invalid or incorrect for the given site.	
-19	Lay aways are not allowed	Attempt to lay away invalid / lay aways are not allowed	
-20	Lay away already stored	Attempt to lay away a transaction where there is already a transaction laid away on that card	Prompt for alternate method of payment
-21	EFT system not configured	The EFT system has not been configured	
-22	Internal error, buffer too small	A buffer is too small	
-23	Unknown comms device type	Invalid / unknown communications device type	Check communications configuration
-24	Configuration file is invalid	Configuration file is invalid / bad format	Check system configuration
-25	No valid accounts	There are no valid accounts specified in the TillInfo.cfg	Check system configuration
-26	Invalid channel	Invalid channel	Check> · 2 transactions aren't being passed down the same channel. · 2 tills aren't using the same channel number. · WinTI EFTChans within the registry has enough available channels set (Socket mode only).
-27	System error –module not loaded	System error (Track2 check module has not been loaded)	
-28	General transaction error		Re-enter transaction
-29	Transaction store unavailable	Transaction store unavailable	Check Live Store. Check hard disk space.
-30	Unspecified error	Unspecified error	Check system log for indication of error.
-31	Unspecified error:2	Transaction cancelled	Channel available for next transaction
-32	Library not open	EFT library is unavailable	
-33	Possible text for error: <fieldname> (<fieldno>) should be X to Y characters in length. <fieldname> out of range, should be X to Y. <fieldname> out of tolerance, is X, should be X +/- Z. Line discount not available for Cendant cards. Line count (X) doesn't match header -> CPC lines (Y). Separate post and packing only on Amex cards. Where <fieldname> = part number, part description, commodity code, unit of measure, quantity, net value, VAT amount, gross value, PAN, PO number,	The error message is made up of a combination of text (1 to 6) with the applicable field name inserted, as applicable. For example: Net value out of tolerance, is 123.45, should be 123.00 +/- 1	

	customer number, customer name, customer VAT no, destination zip, destination country code, order date, original invoice number, cost centre, invoice net amount, invoice VAT amount, post and packing VAT, invoice gross or transaction total. Invalid CPC data		
-34	Modifier field invalid/missing	As the modifier is passed within the T record the host software is likely to be the cause of this	
-35	Invalid card / invalid Track 1	Track 1 is invalid	Re-swipe card
-36	Invalid card / invalid Track 3	Track 3 is invalid	Re-swipe card
-37	Invalid / missing expiry date	The expiry date is either invalid or missing. If key entered, the format should be MMYY	Re-enter expiry date or re-swipe card
-38	Invalid / missing issue number	The issue number is either invalid (value or length) or missing	Re-enter issue number or re-swipe card
-39	Invalid / missing start date	The start date is either invalid or missing. If key entered, the format should be MMYY.	Re-enter start date or re-swipe card
-40	Purchase/refund value bad or missing	The transaction value is either invalid or missing	Re-enter transaction
-41	Cash-back value bad or missing	The cash-back value is either invalid or missing	Re-enter transaction
-42	Auth code value bad or missing	The authorisation code is either invalid or missing	
-43	Cheque account number value bad or missing	The cheque account number is either invalid or missing	Re-enter cheque account number
-44	Invalid cheque sort code	The cheque sort code is either invalid or missing	Re-enter sort code
-45	Invalid / missing cheque number		Re-enter cheque number
-46	Invalid / missing cheque type		Re-enter cheque type
-47	Invalid EFT serial number	The EFT serial number is either invalid or missing in the .Cnf file	Re create *.cnf
-48	Unexpected CPC data	Purchasing card invoice data has been presented for a non-Purchasing Card (where invoice data is not valid/required)	Re-enter transaction without invoice data or prompt for a valid Purchasing Card
-49	Transaction already confirmed or rejected	Attempt to confirm or reject a transaction, which has already been confirmed or rejected	
-50	Copy protection failure	Could be a permission problem on the PC	
-51	Post confirm reversal not allowed for PWCB or Cash Advance (reserved for future use)	Attempt to perform a post confirm reversal on a PWCB or Cash Advance has been dis-allowed (as post confirm reversals are not supported when cash is involved)	Reverse transaction manually (as cash is involved)

-52	Transaction data supplied in post conf rev not consistent with store (reserved for future use)	The details supplied in the post confirm reversal message is not consistent with the data stored for the transaction to be reversed	
-53	Transaction already void	Attempt to perform a post transaction reversal has failed because the transaction has already been voided/reversed	
-54	Card on hot list	The card number is on the locally stored host list (received from the acquirer and/or entered by the customer). The card must be rejected	Prompt for alternate method of payment
-55	Attempt to confirm a declined transaction	The format of the confirmation message is invalid (confirming a declining transaction). The confirmation message should contain a command value of 2 (reverse/reject) and not a value of 1 (confirm).	
-56	EFT_ERR_BAD_CV2	CV2 is invalid	Check CV2 and re-enter
-57	EFT_ERR_BAD_AVS	AVS is invalid	Check AVS and re-enter
-58	Invalid Merchant Details	Merchant Details passed in Web Services Gateway are Invalid.	Check both the GUID and Passcode information that being passed to the Web Services Gateway
-59	Invalid Mobile Number Format	The Mobile Number format passed is incorrect	Please check and re-enter the mobile number supplied.
-60	Invalid/missing bank account number	The bank account number within the supplied T-Record is incorrect.	Check the bank number being passed and re-enter as necessary.
-62	Token does not exist or invalid token for this merchant system	The Token ID supplied is incorrect or invalid for the merchant system	Check the Token ID is correct and for use with the current merchant system
-64	Unexpected / Invalid Authorisation Response	Unexpected / Invalid Authorisation Response from M-Voucher Host	Please contact Verifone Support
-65	Invalid voucher target type	The Target Voucher Type is invalid (M-Voucher)	Please contact Verifone Support
-66	Invalid Refund Pin	The refund pin entered is invalid	Please enter the correct refund pin if continues to fail, please contact Verifone Support
-67	Report Not Supported	The Report ID supplied is either invalid or does not correspond to a report that is supported	Check the Report ID that is being passed
-68	Report Failed	Integrated report failed	Contact Verifone
-69	Gratuity value exceeded	Check Gratuity Value	Check Gratuity Value
-70	Invalid Capture Not Supported	Check PAYware Ocius settings	Capture Method Not Set correctly
-71	Cashback not allowed by card	Card does not allow cashback	Use a different card or proceed without cashback
-72	Cash advance not allowed by card	Card does not allow cash advance	Use a different card
-73	Max refund value exceeded	Refund transaction value is greater than the maximum refund value set on the account	Reduce transaction value
-74	Bill Already Complete	The bill being cancelled is	N\A

		already completed and therefore cannot be cancelled.	
-75	No ETU accounts	Attempt to process ETU transaction without ETU accounts being present on terminal	Contact Verifone
-76	Card is online only	Attempt to process an online only card whilst offline	Check network or use another card
-77	Cancel Failed - In Payment on xxx.xxx.xxx.xxx	Attempt to cancel a lodged Bill failed, usually locked on a specific terminal	Leave for configured amount of time before retrying cancel routine.
-78	Login failed	User ID or PIN is incorrect	Check login details and try again
-79	Confirmation Status Unknown	An invalid confirmation response has been received or the confirmation message to be sent was not saved	
-80	Bill Reference Already Exists	Attempt to lodge a Bill into I-Link that already exists	Clear the original Bill, or re-send this one using an alternative reference.
-81	Print Report Failed	The request report failed to generate or print	Check printer settings, network connection and try again.
-82	Network Error	Error in Network	Check network.
-83	Invalid Record	Invalid Record	The record received is invalid.
-84	PED User already logged in	A Login command has been received, but a user is already logged in	Log the terminal off first, or simply pass a transaction.
-85	PED User not logged in	The terminal needs to be logged in	Send a login command to the terminal, or manually login using the on-screen prompts, then re-send the transaction.
-86	Submission of offline transactions failed	The submission of the offline stored transactions have failed.	The transactions will still be stored on the terminal. Re-try, and if still having problems contact Verifone Merchant Helpdesk.
-87	Problem in network	There has been a problem in the network.	
-88	Voice Referral Timeout	The voice referral transaction has taken too long.	Re-try or cancel.
-89	Invalid Account ID	Invalid Account ID	
-90	Service Not Allowed	Service code not supported	Use another card, or cancel the transaction
-91	Card Not Accepted	Card type not accepted	Use another card, or cancel the transaction
-92	Unknown Card	Unknown card type	Use another card, or cancel the transaction
-93	Not In IIN Range	Unknown card type	Use another card, or cancel the transaction
-94	Application Blocked	The terminal cannot accept this card type	Use another card, or cancel the transaction
-95	Card Blocked	The card has been blocked.	Use another card, or cancel the transaction.
-96	Card Error	There is a problem with the Card	Re-try or use another card.
-97	Authorisation Error	The authorisation process has been interrupted or is not responding.	Check ILink & WinTI are running – or when using gateway, contact Verifone Merchant Helpdesk.
-98	Unknown Client	When using transaction	Configure POS routing for that

	Unknown Transaction Source Unknown Message	processing, if no POS Routing has been configured for the IP Address or File Name where the transaction originates from, ILink does not know where to send the transaction. It therefore rejects it with this message.	Point Of Sale.
-99	Transaction/Bill Cancelled	When a transaction has been cancelled by the user, the system or an ICC card, this error message will be sent.	
-100	Pin Bypass Failed	ICC Card does not allow Pin Bypass.	Use another card.
-101	Invalid Terminal Country Code'	The Terminal Country Code passed is invalid	Please check the ISO Country Codes table and make sure the code being passed is correct.
-102	User has no permissions on specified account	Check account permissions in WebCom.	Please contact Verifone Support
-103	Invalid Currency Code'	The Currency Code passed is invalid.	Please check the ISO Currency Codes table and make sure the code being passed is correct.
-104	Invalid EMV Terminal Type'	The EMV Terminal Type passed is invalid	Please check the EMV Terminal Type that is being passed is valid.
-105	Unknown Message Type	The message type received by server side is not recognised	Please contact Verifone Support
-106	General Enqueue Error	General Verifone Enqueueing Error	Please contact Verifone Support
-107	Transaction Confirmation Error	The transaction confirmation has errored.	Please retry the confirmation and if continues to fail please contact Verifone Support
-108	Payer Auth Error	The Payer Auth has encountered an error.	Please check the error message response and contact Verifone support.
-109	Ukash Auth Error	The Ukash transaction has encountered an error.	Please check the error message response and Contact Verifone Support.
-110	Encryption Failure	An error has occurred in the data encryption.	Please contact Verifone Support
111	Unable to build Auxillary Data Record	The auxillary data record failed to build correctly	Please contact Verifone Support
-112	Transaction rejection error	The attempt to reject the transaction has errored	Please retry the rejection and if continues to fail please contact Verifone support
-113	Unknown Terminal	The terminal\PTID is not recognised	Please contact Verifone Support
-114	Invalid Download Type	The download type is invalid	Please contact Verifone Support
-115	Terminal Registration Failed	The attempt to register the terminal has failed	Please retry the registration if it continues to fail, please contact Verifone Support
-116	Terminal has been deactivated	The terminal has been marked as deactivated.	Please contact Verifone Support
-117	Comms down	Acquirer has been blocked in the database as acquirer is not processing any authorisations (comms down)	Please contact Verifone Support

-118	M-Voucher Service Unavailable	This is when the terminal is in offline mode at the start of a transaction, and cannot connect to the hosted server to allow M-Voucher	Please contact Verifone Support
-119	Barclays Bonus Service Unavailable	Error response when Comms failure between server application and XLS Host experienced.	Please contact Verifone Support
-120	Token Server Error	The Token Server has encountered an error	Please contact Verifone Support
-121	Purchase transaction type not allowed on token	The token provided does not allow purchase transactions	Please supply another token that allows purchase transactions
-122	Refund transaction type not allowed on token	The token provided does not allow refund transactions	Please supply another token that allows refund transactions
-123	Cashback transaction type not allowed on token	The token provided does not allow cashback transactions	Please supply another token that allows cashback transactions
-124	Token expired	The token provided has passed its expiry date	Please register a new token
-125	Invalid TokenID	The token provided is invalid	Please supply another token or contact Verifone Support
-126	Token has no Txn Type Permissions	The Token Registration has no transaction permissions	Please resubmit the token request with transaction permissions enabled
-127	Invalid Token expiration date	The token expiration date provided is invalid	Please resubmit the token request with a valid token expiration date
-128	ProcessingDB Missing or Invalid	The processing database that is passed in the client header is either missing or invalid.	Please check that the message you are sending has the processing database set in the client header and that it is valid (as per the transaction\payer auth request)
-129	Invalid Original Barclays Gift Transaction ID	The Original Gift Transaction ID provided is invalid	Please check the Original Transaction ID and try again.
-130	Invalid Barclays Gift Configuration	Your Barclays Gift Configuration is invalid	Please check the configuration and download to the terminal. If the problem continues please contact support.
-131	Barclays Gift Service Unavailable	The Barclays Gift Service is temporarily unavailable	Please contact Verifone Support
-132	Merchant Reference Required	Your current configuration requires a Merchant Reference to be passed.	Please re-submit the transaction with the Merchant Reference populated.
-133	Account On File Not Allowed	Terminal is operating in offline mode Account does not allow Account On file CNP transactions EFT transaction capture method does not support registration of details for Account On File processing	Please check that the terminal is online Please check the configuration of the account Check the transaction details that you have passed.
-134	Card not allowed to be keyed	The card scheme doesn't allow processing of keyed card numbers	Use another card, or cancel the transaction
-135	Timeout Waiting for Card	A timeout has occurred whilst waiting for the card	Reprocess Transaction.

		and Transactions has been cancelled	
-137	Present Cash Advance Transaction As Purchase	The card presented does not support cash advance and needs to be represented as a purchase txn.	Reprocess Transaction as a purchase
-138	Gratuity Value Incorrect	Check Gratuity Value	Check Gratuity Value
-139	Transaction Timeout	The application has timed out waiting for a Barclays Gift response	Please check whether the gift request has gone through and if necessary please try again.
-140	Schedule Payment registration failed.	The scheduled payment registration has failed.	Please attempt to re-register the scheduled payment or contact Verifone Support
-141	Ocius migration failed	The PAYware Ocius migration failed on the database because the migration has not been setup / enabled	Contact Verifone to arrange for migration
-142	S Record Timeout	Terminal has timeout after 30 seconds from no response from user	Reprocess record if required
-143	Download Failed	The software or configuration download on the V^{x} 810 solution has failed to complete its download successfully.	Please retry the download if it continues to fail please contact Verifone Support
-150	Invalid PayPoint Configuration	The PayPoint configuration that you have setup is invalid.	Please contact Verifone Support
-151	No PayPoint Accounts	There are no PayPoint accounts available.	Please contact Verifone Support
-152	PayPoint Service Unavailable	The PayPoint service is currently unavailable	Please retry the payment or contact Verifone support
-153	PayPoint Download Required	A PayPoint download is required	Please perform a configuration file update to your terminal
-154	PayPoint Account Extraction Failed	PayPoint account file extraction has failed.	Please retry the download if it continues to fail please contact Verifone Support
-155	PayPoint Transaction Type Not Allowed	The PayPoint transaction type provide is not allowed	Please check the Transaction Type supplied and correct
-156	Invalid PayPoint TopUp Type	The PayPoint TopUp type provided is invalid	Please check the TopUp Type supplied and correct
-157	Invalid PayPoint Service Provider	The PayPoint Service Provider provided is invalid	Please check the Service Provider supplied and correct
-158	Invalid PayPoint Scheme	The PayPoint Scheme provided is invalid	Please check the Scheme supplied and correct
-159	Invalid PayPoint Scheme Option	The PayPoint Scheme Option provided is invalid	Please check the Scheme Option supplied and correct
-160	Invalid PayPoint Amount	The PayPoint Amount provided is invalid	Please check the Amount supplied and correct
-161	No PinPad Available	The PIN pad is currently unavailable	Please check the PIN pad is available for use, please contact Verifone Support if the problem persists.
-189	Invalid refund password	An invalid refund password has been supplied during the transaction, and was rejected by the database	Please contact Verifone Support
-999	Token Server Error	Start date or issue data supplied is incorrect or missing	Please check you are passing the appropriate required fields
-1000	Generic Error	Generic Capture Error	Please contact Verifone Support

-1001	Merchant Supplied Bad Data	The information supplied in the post is incorrect	Please check the data that you are sending and retry.
-1002	Bad Source URL	The source URL is unrecognised	Please contact Verifone Support
-1003	Attempting to use a TokenID and a PAN at the same time	A TokenID and PAN were received for the same transaction	Please check the data that is being passed
-1004	Curl Error	Communication Error	Please contact Verifone Support
-1005	Couldn't Extract Error Code from Response	The error code returned could not be extracted	Please contact Verifone Support
-1006	Failed to Retrieve System Config	Payment Page has failed to retrieve your System Configuration	Please contact Verifone Support
-1007	Unusual Data Supplied (Possible Attack)	The data that has been supplied is suspicious	Please check the data that you are sending and contact Verifone support
-1008	Failed to Retrieve Session Data	Payment Page has failed to retrieve your session data	Please retry the payment or contact Verifone support
-1009	Failed to Create New Session	Payment Page has failed to create a new session	Please retry the payment or contact Verifone support
-1010	Bad SessionID received from end user	The sessionID provided by the front end is incorrect.	Please check the data that you are sending and retry.
-1011	Bad PIN received from end user	The PIN provided by the front end is incorrect.	Please check the data that you are sending and retry.
-1012	Session Finished	The session that you are trying to use has already finished.	Please retry the payment or contact Verifone support
-1013	Failed to extract PA Data	An error has occurred trying to decrypt\extract the Payer Auth data	Please retry the payment or contact Verifone support
-1014	Session Expired	The session that you are trying to use has expired.	Please retry the payment or contact Verifone support

ADDRESS VERIFICATION SYSTEM RESULTS

When processing transactions on a terminal with AVS checking, there are different results produced dependent upon which checks have been matched. Here is a table to describe the results more accurately:

CV2 RESULT	POST CODE RESULT	HOUSE NUMBER RESULT	OVERALL AVS/CV2 RESULT DISPLAYED ON TERMINAL
Match	Match	Match	“Data Matched”
Match	Match	No Match	“Sec Code Matched”
Match	No Match	N/A	“Sec Code Matched”
No Match	Match	Match	“Address Match Only”
No Match	Match	No Match	“Data Not Matched”
No Match	No Match	N/A	“Data Not Matched”
Add On Not Enabled/ Not Supported By Acquirer	Match	Match	“Address Match Only”
Add On Not Enabled/ Not Supported By Acquirer	Match	No Match	“Data Not Matched”
Add On Not Enabled/ Not Supported By Acquirer	No Match	N/A	“Data Not Matched”
Not Checked	Match	Match	“Address Match Only”
Not Checked	Match	No Match	“Data Not Matched”
Not Checked	No Match	N/A	“Data Not Matched”

CONTACT DETAILS

VERIFONE SERVICES UK & IRELAND

100 Eureka Park
Ashford
Kent
TN25 4AZ

PAYWARE OCIUS MERCHANT HELPDESK

T: 08444 828 222
E: Ocius.helpdesk@verifone.com

TECHNICAL SERVICES

T: 08444 828 273
E: Ocius.techservices@verifone.com

CUSTOMER SERVICES

T: 08444 828 268

SALES ENQUIRIES

T: 08444 828 203
E: Ocius.enquiries@verifone.com

verifone.co.uk