First Data Merchant Solutions
EMEA Payment Gateway

Virtual Terminal & Online Portal

User Guide

Version 2.1

Version Control

Version Number	Issue Date	Description of Change
2.0		New Edition
2.1		Revised Edition

Table of Contents

1 Introduction

The First Data EMEA Virtual Terminal (VT) is an easy way for merchants to process monetary transactions via the Internet by turning any Personal Computer (PC) into a Point of Sale (POS) terminal.

At the same time it provides access to an Online Portal which is one central, secure location where you can manage everything related to transaction processing:

- Run secure transactions yourself
- Set up your web site to run transactions for you
- Prevent fraud
- Review transaction reports

Process Transactions the Way You Want - From Anywhere

The Virtual Terminal offers functions in a similar way to terminals commonly used at retail stores. You simply enter the data needed for the VT transaction and go. It can even take care of recurring transactions (if you sell subscription services, for example).

The terminal is completely customisable, allowing you to show only what you need to run your business efficiently. Other than a small number of fields that are necessary for a particular transaction type (e.g. Card number for a Card transaction), you will be able to select exactly what you want to appear on the page; because it runs via the Internet, you can log on from anywhere you can get Internet access, giving you instant access to process orders from wherever you are.

Manage Your Internet Payment Gateway Account

The Online Portal allows you to manage everything from one place.

The **Reports** section is where you view your transaction reports, charts and graphs, helpful for business visualisation and presentations. You can even view consolidated reports for multiple stores by setting up a multi-store reporting structure. (A separate multi-store administrative account login is required for multi-store reports. Contact support to get your initial multi-store admin login ID and password.)

The **Administration** section is where you turn to change your password, set your fraud settings, manage your users or set up your multi-store reporting structure. (A separate multi-store administrative account login is required for multi-store reports. Contact support to get your initial multi-store admin login ID and password.)

The **Customisation** section lets you customise your Virtual Terminal pages, turning it into a simple mail-order/telephone-order system, a recurring transaction processor, or your own custom terminal.

Access Administration and Customisation Functions

The Online Portal also allows you to access functions you need to set up and customise the integration of your web shop with our FDMS EMEA Connect solution. You can access these functions via the Customisation section.

To protect your account, we encourage you to log out of the Virtual Terminal by clicking on the **Logout** link at the right top of the page when leaving your computer. You will also be logged out automatically after a period of inactivity.

1.1   Pre-Requisite

The following checklist shall provide an overview enabling you to make sure that you have received the whole set when registering your application for the First Data EMEA Virtual Terminal and Online Portal:

- *Client Certificate p12 File:* The client certificate stored in a *p12* file having the naming scheme **storeID.p12**, e.g. if your store id is 1120541234, your client certificate file will be **1120541234.p12.** This file is used for authenticating the client at the Payment Gateway.
- *Store ID:* Your store ID (e.g. *1120541234*) which is required for authentication.
- *User ID:* The user ID denoting the user who is allowed to access the Virtual Terminal, this is required for authentication.
- *Password:* The password required for the basic authorization.

Contact the Technical team (see section 1.2) if you have not yet received the above details.

The First Data Virtual Terminal can be accessed from all major browsers once you have all the above listed credentials and have successfully installed the Client Certificate *.p12 in the browser you'd like to use to access the Virtual Terminal URL.

See Appendix A for a step by step guide on how to install Client Certificate.

1.2   Technical Support

This Guide contains the information required for processing transactions with the FDMS EMEA Virtual Terminal and using the Online Portal.

Technical support is available via email and telephone call coverage from 09:00 to 17:00 Monday to Friday (UK time).

Email: fdmsIPGConnect@firstdatacorp.co.uk

Telephone: 01268 567 137

Web: https://www.firstdatams.co.uk/fdms/en_gb/home.html

2 Transaction Types

This section briefly describes the available transaction types in the FDMS EMEA Virtual Terminal to enable you farmiliarise yourself with the terminology and to use the appropriate transaction type for your orders and returns (refunds). Please note that no funds are transferred during any of the following listed transaction types. Funds are transferred only after your batch of transactions is settled (this is set up to occur automatically once a day).

2.1 Sale

A sale transaction type immediately charges a customer's card or bank account.

2.1 Authorise Only

An "Authorise Only" reserves funds on a customer's card. "Authorise Only" does not charge the card until you perform a Completion (Ticket Only) transaction and/or confirm shipment of the order (using an option available in "Reports"). Note that authorisation reserves funds for varying periods, depending on the issuing Card Company's policy. We strongly suggest that you confirm shipment as soon as possible after Authorisation.

2.2 Completion

Completion (Ticket Only) is a post authorisation transaction. This transaction captures the funds from an Authorise Only transaction (see Section 2.2), reserving funds on the customer's Card for the amount specified. Funds are transferred when your batch of transactions is settled. If you enter a larger total in the Post-Authorisation transaction than was specified for the *Authorise Only* transaction, the *Post-Authorisation* transaction may be declined. If you enter a smaller amount than was authorised, an adjustment is made to the Authorisation to reserve only the smaller amount of funds on the customer's Card for the transaction.

2.3 Forced Ticket

A Forced Ticket transaction type is used in a similar way to a *Completion* transaction, except it is specifically for authorisations you obtained over the phone. It requires a reference number (or approval code) that you should have received when you carried out the phone authorisation.

2.4 Return (Refund)

Returns funds to a customer's Card against an existing order on the First Data EMEA Payment Gateway. To perform a return (refund), you need the order number (which you can find in your Reports). If you perform a Return of the full order amount, the order will appear in your Reports with a transaction amount of 0.00. To perform a Return transaction, use the *Return* page.

2.5 Credit

Credit returns funds to a customer's Card for orders outside the First Data Payment Gateway. Use the Credit page to perform a *Credit* transaction. Credit transactions are marked as *Returns* in your Reports.

2.6 Void

This function enables you to cancel/void previously authorised transactions. Transactions can only be voided before the batch of transactions is settled.

3 Virtual Terminal Point of Sale

Once logged in the Virtual Terminal, the main page presented is the Point of Sale (POS).
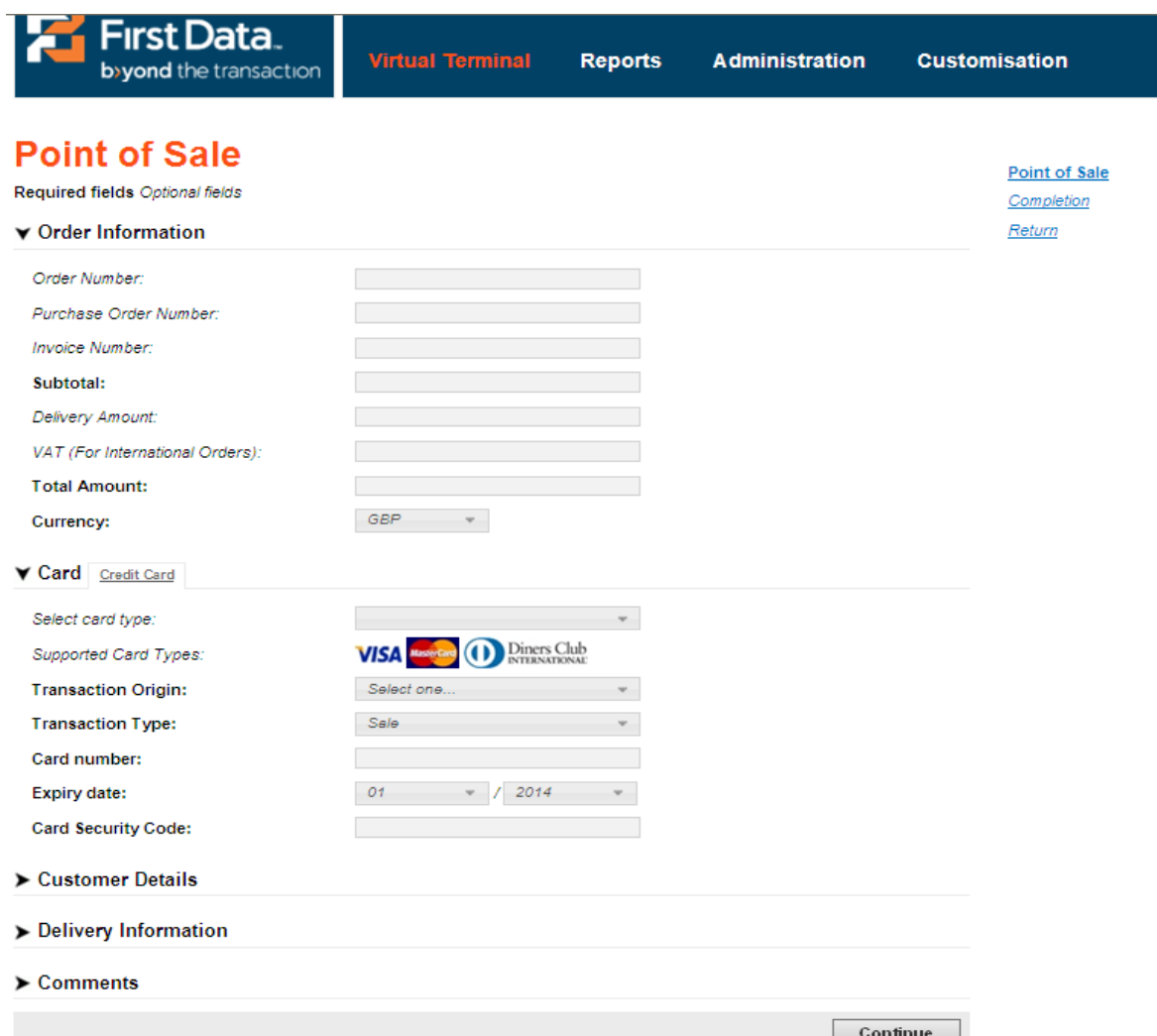
The *Transaction Type* drop down menu within the POS are *Sale, Authorise Only* (Pre-Authorisation) and *Forced Ticket* (Referral).

Other transaction types e.g. *Completion* and *Return* (Refund) will be listed on the top right hand corner of POS page (note these transaction types require a look up in the database to get order information).

A hide/reveal function is available for all sections of the page, which can expand to provide additional options or fields - such items are identified by a right-arrow graphic. When clicked upon, the arrow changes to point downward and the expanded choices are revealed. Clicking again reverses the process.

NB: Contact the technical support team (See Section 1.2) if you require the *Transaction Type Credit*.

Virtual Terminal Point of Sale screen-print:

The following sections will describe the fields in the Virtual Terminal Point of Sale.

3.1 Order Information

The Order Information section has the following mandatory fields:

Total Amount (sum of VAT and Delivery) *Currency*. The fields under Order Information are described below:

- **Order Number (Optional):** This is an optional field. If you wish to assign an order number to the transaction, enter one in the text box provided. Each order number must be unique, so if you are going to use this field on a regular basis, you should adopt an order number generation procedure. If you choose not to assign an order number, the First Data system will automatically generate one for you.
- **Purchase Order Number (Optional):** This is an optional field. If there is a purchase order number associated with the transaction, enter one in the text box provided. You may have several transactions against the same purchase order, you may use the same purchase order number for several transactions, if needed.
- **Invoice Number (Optional):** This is an optional field. If there is an Invoice Number associated with the transaction, enter one in the text box provided.
- **Subtotal (Optional):** This is an optional, once *Total Amount* is entered this field will automatically populate. If you have a sub total amount for the order, enter one in the text box provided. This field only accepts numeric data.
- **Delivery Amount (Optional):** This is an optional field, if you have a delivery amount for the order (e.g. Shipping charges) enter one in the text box provided. This field only accepts numeric data.
- **VAT (For International Orders):** This is an optional field. The field can be used by merchants involved in international business where you need to charge a Value Added Tax (VAT), either in addition to or in lieu of the regular sales tax. If the Value Added Tax applies to your order and if you need to charge the customer the VAT now, enter the amount of the VAT in the VAT field. In some cases, you may not need to charge the VAT; it will be taken care of when the goods are imported.
- **Total Amount (Required):** This is a mandatory field. If you enter Subtotal, Delivery Amount and VAT, the Virtual Terminal will automatically calculate the total amount for you. If you need to, you can replace this value with any real or integer number representing the total amount of the transaction. The total amount should include tax, VAT (if applicable), and shipping charges, and should reflect the sum of all charges for this transaction. The total amount should always equal the sum of the product subtotal, tax, shipping, and VAT. This is a required field for ALL transactions.
- **Currency (Required):** This field will list the currency set-up on your merchant account with First Data, if you wish to accept a currency not listed please contact the technical team (See Section 1.2).

3.2 Card Information

The Card Information section has the following mandatory fields for both Credit and Debit cards:

Transaction Origin; Card number; Expiry date and Card Security Code. The fields under Card are described below:

- **Select card type:** The drop down menu shows a list of the supported card types on your merchant account. Select the appropriate card type for the order.
- **Supported Card Types:** A graphic for each card type that has been setup for your store is shown, by selecting the brand the card type is automatically selected
- **Transaction Origin (Required):** Three options are presented in the drop down menu:

  - Mail Order/Telephone Order
  - Retail (face to face)
  - Electronic Commerce (internet.

Your Virtual Terminal is configured to only accept *Mail Order/Telephone*. Please ensure you select *Mail Order/Telephone Order* when processing an order.

- **Transaction Type (Required):** Card Payment Details section shows fields required for a Card Sale, Authorise Only, or Forced Ticket transaction.
- **Card number (Required):** This field accepts the long card number.
- **Expiry date (Required):** Select the Card Expiry Date in the drop down menu
- **Card Security Code:** This field accepts the 3-4 digit security code at the back of the card.

3.3 Customer Details

All the fields in Customer Details are optional. If your business require customer details (Billing Information) please complete this fields accordingly. The fields are listed below:

- **Customer ID:** Assign an ID for the Customer
- **Customer Name:** Customer Name
- **Billing Company:** Billing Company.
- **Address:** Billing Address line 1.
- **Address(2):** Billing Address line 2.
- **Town/City:** Town/City of cardholder
- **State/Province:** State province of cardholder
- **Country:** Select country from drop down menu
- **Post Code:** Post Code of Cardholder
- **Phone:** Phone number
- **Fax:** Fax number
- **Email:** Email address

3.4 Delivery Information

All the fields in Delivery Information are optional. If your business requires delivery information (Shipping Information) please complete this section accordingly. The fields are listed are below:

- **Name:** Customer Name
- **Address:** Shipping Address line 1.
- **Address(2):** Shipping Address line 2.
- **Town/City:** Town/City of cardholder
- **State/Province:** State province of cardholder
- **Country:** Select country from drop down menu
- **Post Code:** Post Code of Cardholder

Note: If you wish to make any of the above fields mandatory in your Virtual Terminal Point of Sale, follow the steps outlined below prior to accepting payments.

1. Go to *'Customisation'*
2. Go to *'Customise your Virtual Terminal page content'*
3. Expand *'Customer Details'* and/or Delivery Information.
4. Tick the *'Required'* checkbox of the field names you wish to make mandatory.
5. Click on Submit.

3.5 Make Recurring Payment

All the fields in *Make Recurring (For Credit Card Sale Transactions ONLY)* are mandatory if you wish to initiate a recurring Card (Sale) transaction.

- **Make Recurring?:** Click 'Yes' if you want to set-up a recurring transaction
- **Bill The Customer:** Specify billing period.
- **Start On (MM/DD/YYYY):** Specify start date- initial payment.
- **End After:** Specify number of counts for payment.

To initiate a recurring transaction see section 4.5 of this Guide

3.6 Comments

This field is optional, you can use this field to enter optional notes about the transaction.

Comments are visible in your Reports, so they can help you with your transaction management if you use them effectively.

3.7   Continue (Submit Order)

Once completing all the optional and mandatory fields in the Virtual Point of Sale the '*Continue*' button, takes you to the next screen/stage of the order processing.

When you click the Continue button, all your entries are validated. If pieces of information are missing or incorrect, the First Data Virtual Terminal page will reappear with an error message at the top and the incorrect or missing fields flagged with an error graphic. If this should occur, make the appropriate corrections to the fields, and then click the '*Continue*' button again.

If there are no apparent invalid entries, a review of all the information you entered with a request for confirmation will appear. Review the information and, if necessary, click on Back and make any corrections. Otherwise, click on '*Submit*'.

The Transaction Result screen will appear. The result screen will contain all the information you entered, plus an extra section at the top called Transaction Information.

See Appendix B of this Guide for full description of an FDMS Approval Code.

3.8   Show Receipt (Print Receipt)

The Show Receipt enables you to print transaction receipt.

To print receipt follow the steps outlined below:

1   Click on the Show Receipt button at the bottom of the Transaction Result page. A new browser window will open with a transaction receipt.
2   Click on the Print Receipt button at the bottom of the Receipt page to print the receipt.
3   Once you have printed all the receipts you need, close the receipt window by clicking on the Close button at the bottom or on the X in the top right hand corner of the Receipt window.

4 Processing Virtual Terminal Transaction Types

4.1 Processing Sale

To perform a Sale transaction, go to the First Data Virtual Terminal Point of Sale and follow the steps outline below:

1. If using the product catalogue feature, select items from the Product Catalogue (See Section 7.3 of this Guide on how to set-up Product Catalogue)

2. Enter Order Information (note: Order Number is optional, the Gateway will assign if you don't enter, however, if you require your own Order Number, it has to be unique for every transaction

3. Select Card Type

4. Select Transaction Origin (always select **Mail Order/Telephone Order**)

5. Enter Card Information (See Section 4.1.1 for additional information)

6. Select Transaction Type *Sale*

7. If needed, enter further optional fields (e.g. Customer details and Delivery Information)

8. Click on the *Continue* button

9. If there are data entry errors or any missing required fields, the same page will reappear with an error message at the top, and all incorrect/missing fields flagged with a warning graphic. Make any necessary corrections, and then click the *Continue* button again. Once your page is error free, a *Please Confirm* page will appear.

10. Review the data, make corrections if needed by clicking on the Back button, then click the Submit button. A Transaction Result page will appear.

11. Review the Results.

Note: For security reasons, you will be logged out of the Virtual Terminal when you attempt to take a payment after 30 minutes of inactivity. First Data highly recommend you refresh your browser prior to taking payment if you are not sure how long you have been inactive.

4.1.1 Card Security Code information

Mail Order and Telephone Order (MO/TO) and other Card-Not-Present transactions have higher fraud rates than Face-to-Face (Cardholder Present) transactions. To help reduce fraud in the Card-Not-Present environment, card companies have introduced a card code programme.

Visa® calls this code *Card Verification Value (CVV)*; MasterCard® calls it *Card Validation Code (CVC)*; American Express calls it *4DBC*.

The card security code is a three- or four- digit security code that is printed on the back of cards (American Express: front of the card). The number typically appears at the end of the signature panel. This program helps validate that a genuine card is being used during a transaction.

To help combat fraud, Card-Not-Present merchants should always enter a card security code (if on the card) when processing an authorisation.

You enter the card code on the Point-of-Sale screen when processing an order (See the Virtual Terminal POS screen print in Section 3 above). First Data then compares the card code against the code on file with the card-issuing bank. Results of this comparison show in the transaction approval code.

See Appendix B of this Guide for detailed description of an FDMS Approval Code.

4.2   Processing Authorize Only (Pre-Auth)

To perform an Authorise Only transaction (Pre-Auth), go to the First Data Virtual Terminal Point of Sale and follow the steps below:

1   If using the product catalogue feature, select items from the Product Catalogue (See Section 7.3 of this Guide)

2   Enter Order Information (note: Order Number is optional, the Gateway will assign if you don't enter, however, if you wish to enter an Order Number, it has to be unique for every transaction

3   Select Card Type

4   Select Transaction Origin (always select **Mail Order/Telephone Order**)

5   Enter Card Information

6   Select Transaction Type *Authorize Only*

7   If needed, enter further optional fields

8   Click on the *Continue* button

9   If there are data entry errors or any missing required fields, the same page will reappear with an error message at the top, and all incorrect/missing fields flagged with a warning graphic. Make any necessary corrections, and then click the Continue button again. Once your page is error free, a Please Confirm page will appear.

10 Review the data, make corrections if needed by clicking on the Back button, then click the Submit button. A Transaction Result page will appear.

11 Review the Results.

Note: *Authorise Only* transaction reserves funds on a customer's credit card. Authorise Only does not charge the Card until you perform a Completion (Ticket Only) transaction and/or confirm shipment of the order (using an option available in Reports). Note that authorisation reserves funds for varying periods, depending on the issuing Card Company's policy. We strongly suggest that you confirm shipment as soon as possible after *Authorisation*.

4.3 Processing Completion (Post-Auth)

Running an *Authorise Only* transaction (See section 4.2) tells you whether the customer has sufficient funds on the card for your order, but it may or may not reserve any funds for you.

After you run an Authorise Only transaction, you need to complete it in order to reserve the funds (this transaction is sometimes referred to as a post authorisation).

To complete a pre-auth, go to the First Data Virtual Terminal Point of Sale and follow the steps below:

1   Click on '***Completion***' (top right hand corner of the Point of Sale page)

2   The first Completion page simply asks for the order number. This is the order number associated with your Authorise Only transaction (See section 4.2). If you do not know your Order Number:

   a. Go to *Reports*.

   b. Go to *Orders* or *Transactions* and select a search criteria for the *Authorise Only* transaction.

   c. Look for the Order Number at the column labelled *Order#* in the reports table.

3   Once you've located the order number, enter it in the input box (step 2 above), then click on the *Retrieve Order* button.

4   A new page (Completion) will appear with several pre-filled input fields related to the order. Review these fields to ensure you have selected the correct order. (You may have to expand some of the sections at the bottom of the page to see all the fields you need to see.) If this isn't the right order, click on the Back button on your browser and enter the correct order number to retrieve. If it is the right order, make any changes you need to make to the input fields, and then click on the Continue button.

5   Once you click the Continue button, if all entries in the form were valid, another page will appear asking you to confirm the information.

6   If you are happy with the data, click on the Submit button; otherwise, click on the Back button to make the appropriate changes. (If any fields are missing or incorrect, the Completion page will reappear with an error message at the top and the incorrect/missing fields flagged with a warning graphic. Make the appropriate changes then click Continue

7   Review the information, and then click the Submit button. A final Transaction Results page will appear, indicating whether the transaction was approved or declined and reiterating all the transaction information.

NB: You can also perform completion once you get to step 2(c) above. Click on the Order number of the transaction you wish to *Complete* and the Order Details will appear given you the option '***Please enter amount for completion***' check details, enter amount and click Completion.

4.4   Processing Forced Ticket (Voice Auth)

Use a *Forced Ticket* transaction to complete the Sale for an authorisation you received over the phone.

To perform a Forced Ticket transaction (this transaction is sometimes referred to as Voice Auth or Referral), go to the First Data Virtual Terminal Point of Sale and follow the steps below:

1   If using the product catalogue feature, select items from the Product Catalogue (See Section 7.3 of this Guide).

2   Enter Order Information

3   Select card type

4   Select Transaction Type **Forced Ticket**

5   A Reference number field will appear. Enter the card details and the reference number (the authorisation code you received over the phone)

6   If needed, enter further optional fields

7   Click on the Continue button

8   If there are data entry errors or any required fields are missing, the same page will reappear with an error message at the top, and all incorrect/missing fields flagged with a warning graphic. Make any necessary corrections, and then click the Continue button again. Once your page is error free, a *Please Confirm* page will appear.

9   Review the data, make corrections if needed by clicking the Back button, then click the Submit button. A Transaction Result page will appear.

10 Review the Results.

4.5   Processing Recurring Transaction

If you have an agreement with your customer to set them up for recurring payments for daily, weekly, monthly or yearly, you can use the '*Make Recurring (For Credit Card Sale Transactions ONLY)'*.

To initiate a recurring transaction, go to the First Data Virtual Terminal Point of Sale and follow the steps below:

1   If using the product catalogue feature, select items from the Product Catalogue (See Section 7.3 of this Guide).

2   Enter Order Information (note: Order Number is optional, the Gateway will assign if you don't enter one, however if you wish to enter an Order Number it has to be unique for every transaction.

3   Select Card Type

4   Select Transaction Origin (always select **Mail Order/Telephone Order**)

5   Enter Card Information

6   Select Transaction Type

7   If needed, enter further optional fields

8   Click on the '*Make Recurring?' Yes* checkbox.

9   Enter how often you wish to charge the customer. In the '*Bill The Customer*' fields, enter a number from 1 to 999 with no decimal point and select day, week, month, or year in the dropdown box. For example, if you wish to charge the customer once a year, enter the number 1 and select "year" in the dropdown box. To charge the customer twice a year (once every 6 months), you would enter the number 6 and select "month" in the dropdown box.

10   Select the month / day / year to start charging the customer in the 'Start On' (MM/DD/YYYY)' field dropdown boxes.

11   Enter the number of times to charge the customer in the '*End After*' textbox.

12   If there are data entry errors or any missing required fields, the same page will reappear with an error message at the top, and all incorrect/missing fields flagged with a warning graphic. Make any necessary corrections, and then click the Continue button again. Once your page is error free, a Please Confirm page will appear.

13   Review the data, make corrections if needed by clicking on the Back button, then click the Submit button. A Transaction Result page will appear.

14   Review the Results.

4.6   Processing Return (Refund)

If you wish to refund a transaction previously authorised should a customer return something associated with an order, you can credit their account for the amount of the return using a Return transaction.

To initiate a return (Refund), go to the First Data Virtual Terminal Point of Sale and follow the steps below:

1   Click on '***Return***' (top right hand corner of the Point of Sale page)

2   A page will appear, with a field for the order number. If you don't know your order number, you can find it in your Reports.

a.   Go to Reports.

b.   Go to Orders or Transactions and select a search criteria for the transaction.

c.   Look for the Order Number at the column labelled Order# in the reports table.

3   Locate the order number, enter it in the input box (step 2 above), then click on the *Retrieve Order button*. A page will appear showing all the existing information from that order.

4   Review these fields to ensure you have selected the correct order. (You may have to expand some of the sections at the bottom of the page to see all the fields you need to see.) If this isn't the right order, click on Back button to return to the previous page and retrieve an alternate order.

5   If this is the correct order, enter the amount to return in the '*Transaction amount*' field. By default, the fields will be pre-filled with the total amount available to be returned. Amend as appropriate.

6   Once you've finished with the Order fields, change any other fields related to Customer Contact Information, Payment Information, or Comments, and then click the Continue button.

7   Once you click the Continue button, if all entries in the form were valid, another page will appear asking you to confirm the information.

8   Click on the Submit button if you are happy with the details; otherwise, click on the Back button to make the appropriate changes, and then click the Submit button.

9   A final Transaction Results page will appear, indicating whether the transaction was approved or declined and reiterating all the transaction information.

NB: You can also perform Return (Refund) once you get to step 2(c) above. Click on the Order number of the transaction to be refunded and the Order Details will appear given you the option '***Please enter amount to be returned***' check details, enter amount and click Return Order.

4.7   Processing Credit

This functionality shall be used if you wish to credit a customer account for an order/transaction that occurred outside the First Data Internet Payment Gateway.

This function may not be available for your merchant account.

If you do not see the Credit function listed in the Side Menu Box of your Virtual Terminal Point of Sale, you do not have permission to perform a credit.

Contact the First Data technical team (see section 1.2) if you require this and do not have it.

To initiate a Credit, go to the First Data Virtual Terminal Point of Sale and follow the step below:

1   Click on '***Credit***' (top right hand corner of Point of Sale page)

2   Credit page will appear, complete the Total Amount to be credited and enter the card details to be credited, you can complete the additional optional fields and click continue.

3   Once the entries are validated, a confirmation page shall appear.

4   Review and click on the Submit button if you are satisfied with the entry, else, click on the *Back* button to make the appropriate changes. (If any fields are missing or incorrect, the Credit page will reappear with an error message at the top and the incorrect/missing fields flagged with a warning graphic. Make the appropriate changes then click the *Continue* button again.

5   A confirmation page shall appear. Review the information, and then click the Submit button. A final Transaction Results page will appear, indicating whether the transaction was approved or declined and reiterating all the transaction information.

4.8   Processing Void

The *Void* functionality shall be used if you wish to void an order which has not yet been settled.

To void an order, follow the steps below:

1   Click on '***Reports***' (on the top menu bar)
2   If you wish to void credit card orders, click on the View Credit Card Batches link in the Side Menu Box
3   Specify Time Period:—Select any of the named time periods or enter a specific range of dates.
4   Click on the *Submit Query* button. The batch report will appear.
5   Click on the words *Current Batch* to bring up the Current Batch report
6   Select the order(s) you wish to void by clicking on the corresponding checkboxes in the left-most column.
7   Click on the *Void Selected Transactions* button at the bottom of the page.
8   A page showing the results will appear. Each order you chose to void should show on the list.

5 Virtual Terminal Reports
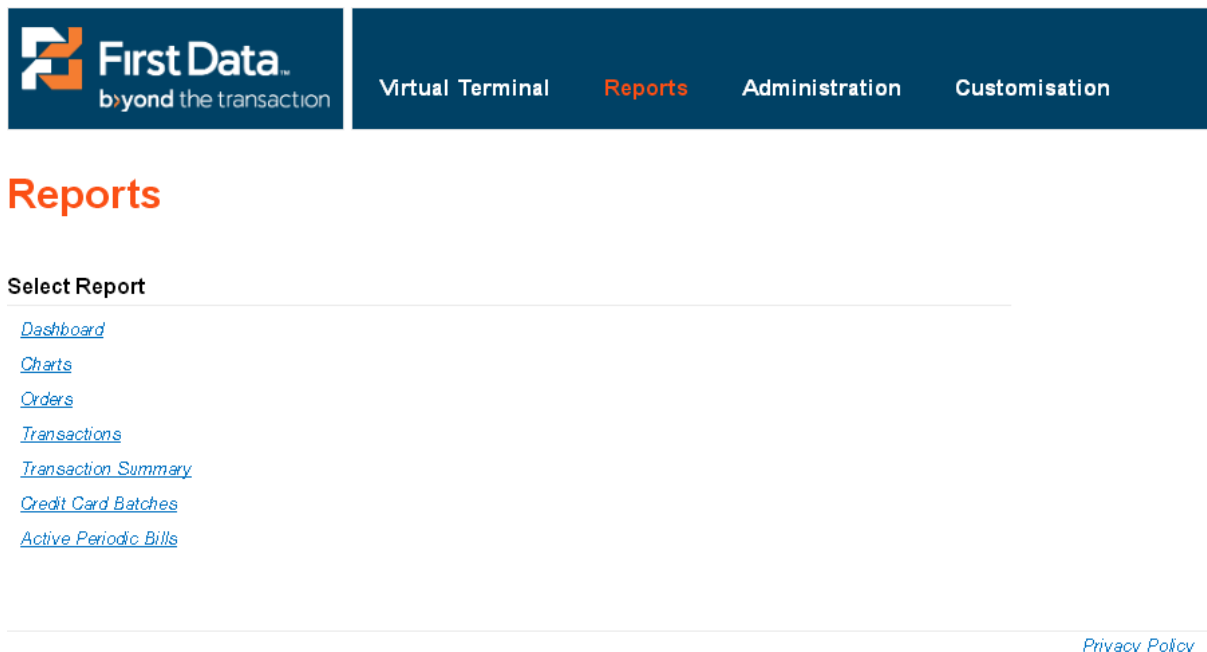
The Virtual Terminal Reports can be used to view your store's transactions from several different perspectives and to perform some administrative tasks.

To view the reports, click on the Reports button on the Main Menu Bar.

The Reports Main Menu for your store is displayed in the Side Menu Box and in the main content portion of the screen. The reports available are listed below.

- **Dashboard**—shows information on card sales made including a table with the last 6 months transactions
- **Charts**—shows transactions in bar, pie, or line charts.
- **Orders**—shows all successful orders by specific time period, by credit card number and time, by order number, or by user ID and time. You also have the option to show only unshipped orders.
- **Transactions**—shows all transactions by time period, by credit card number and time, order number, User ID and time or by transaction type and time.
- **Transaction Summary**—shows a summary of approved and declined AUTH and SALE transactions and a summary of approved AUTH and SALE transactions by card type.
- **Credit Card Batches** —lets you view credit card batches processed during a specified time period.
- **Active Periodic Bills**—shows information about recurring transactions and allows you to modify them.

Screen print of Reports page:

Credit Card Numbers

As a security feature, only the first four and last four digits of credit card numbers are displayed in the reports. These Credit Card Identification (CCID) numbers are often active links that can be selected to display information about all transactions involving the selected card number.

Downloading Report Data

To download the data from any of the reports for use with your own accounting tool, follow the steps below:

1   Bring up the report which contains the data you wish to download.
2   Locate the *Export All Data* button located at the bottom of the page.
3   Select your desired format from the dropdown list. Choose either CSV (Comma delimited) or XML format. CSV lists are suitable for importing into most common spreadsheets or databases. XML format is helpful for applications that allow you to import XML.
4   Click on the Export All Data button to download the data. Depending on your browser, a File Download dialogue box will most likely appear, asking what you would like to do to the file (Open, Save, or Cancel). If you choose Open, the file will open in the application that is assigned to that type of file. Choosing Save will ask you to choose a location where you wish to save the file.

Regardless of the number of pages in the report, all report data will be included in the downloaded file.

The following sub sections will describe how to access and use the reporting tools listed above.

5.1 Dashboard Report

To view the Dashboard click on the Reports button in the Main Menu Bar then click on Dashboard.

The Dashboard offers a graph showing the following:

- Past weeks Processed Sales Volumes
- A chart showing the past 3 months of **Transactions by status** (approved versus declined)
- A **Transaction overview** table offering details of the last 6 months transactions.

The Transaction overview table can be sorted by clicking on any of the headers and there is a search option to search for a specific transaction if required.

The details of each transaction can be viewed by clicking on the transaction's *Order* reference.

A new window will then provide you with the Order Detail Report. Please see 5.3 Order Detail Report for what can be viewed and managed from this report.

There is also an option to select to '*Make the Dashboard your VT start page*'.

A sample screen print of Dashboard:
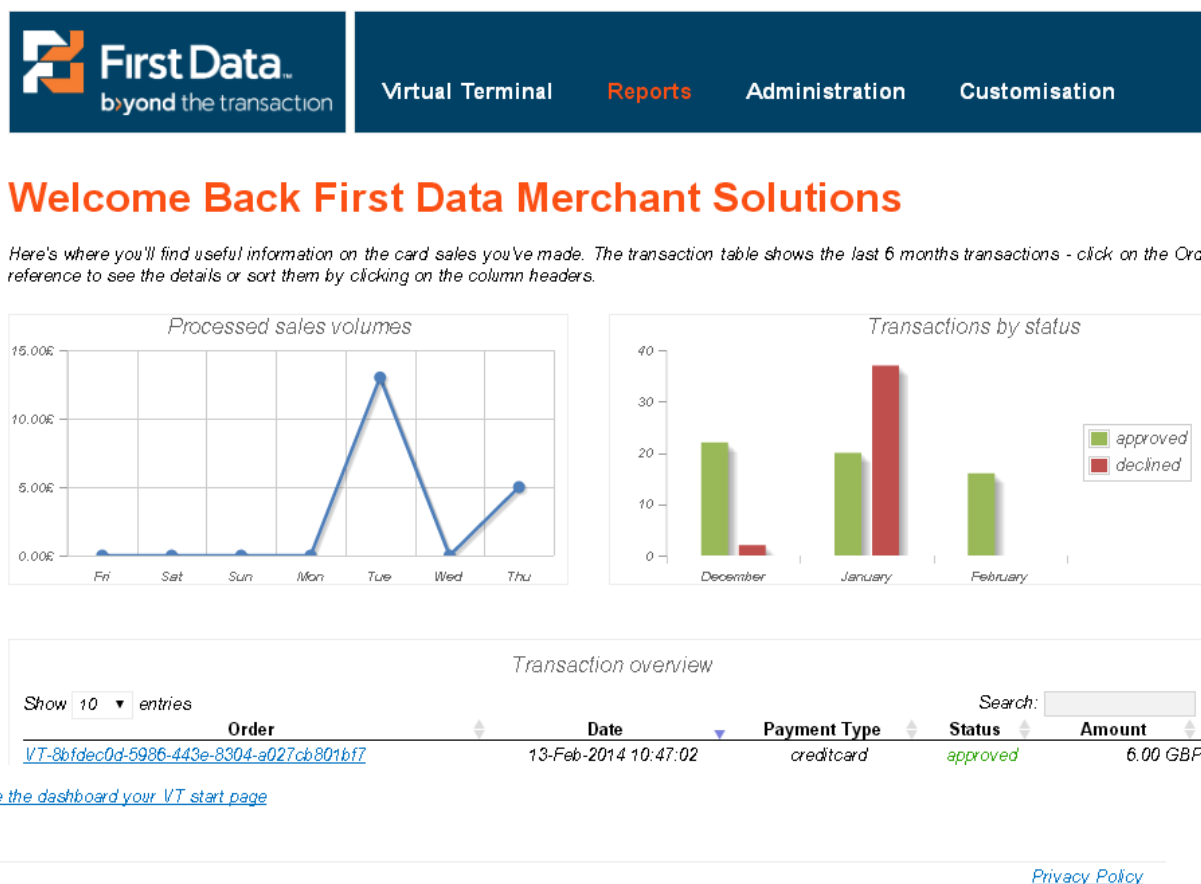
5.2 Charts Report

The First Data Internet Payment Gateway offers four graphical chart types, which are helpful for visualising orders and sales, and for when you need charts for a presentation.

To view your orders in chart format, follow the steps below.

1   Click on the Reports button in the Main Menu Bar

2   Click on *Charts* link in the Side Menu Box. The View Transaction Charts screen appears.

3   Select Chart Type: select an option. You can view your transactions in the following

    a.   Bar Chart Detail

    b.   Pie Chart

    c.   Strip Chart

    d.   Bar Chart Summary

4   Select Transaction Types: select any of the listed transaction types or click on the "All" checkbox in the separator bar if you would like to view all the transaction types.

5   Specify Time Period: select any of the named time periods or enter a specific range of dates you wish to view.

6   Select Hierarchy: choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)

7   Click on the Submit button to view the report. If you want to re-enter the information, click on the Reset button to clear the information.

A sample screen print of Dashboard:

5.2.1 Chart Types

Depending on which type of chart you chose, the chart which appears will look different.

The chart types available are listed below:

- **Bar Chart Detail**

  The Detailed Bar Chart report shows the transaction totals by type in a bar chart format. Each transaction type is shown in a different colour. For each month in the specified timeframe, there is a row of coloured bars showing transaction totals for that month. At the bottom of the chart, a table shows summary statistics for each type of transaction. Hold your mouse over any coloured bar to see the total exact amount of transactions of that type. Clicking on the bar will bring up a detailed Transactions Processed report for that transaction type. (For more information on viewing detailed transaction reports, see Viewing Transactions.) Click on the coloured boxes in the legend on the right to see individual bar chart reports for the selected transaction type. Right click on any of the charts to save that chart as a graphic in jpeg format. You can then import the graphic into your presentations or documents as needed.

- **Bar Chart Summary**

  The Summary Bar Chart report shows the transaction totals by type in a bar chart format. Each transaction type is shown in a different colour. Each coloured bar represents the total amount of all transactions of that type over the entire timeframe specified. At the bottom of the chart, a table shows summary statistics for each type of transaction. Hold your mouse over any coloured bar to see the total exact amount of transactions of that type. Clicking on a coloured bar will bring up a detailed Transactions Processed report for that transaction type. (For more information on viewing detailed transaction reports, see Viewing Transactions.) Right click on any of the charts to save that chart as a graphic in jpeg format. You can then import the graphic into your presentations or documents as needed.

- **Pie Chart**

  The Pie Chart report shows the transaction totals by type in a pie chart format. Each transaction type is shown in a different colour. At the bottom of the chart, a table shows summary statistics for each type of transaction. Hold your mouse over any coloured pie piece to see the total exact currency amount of transactions of that type. Clicking on a pie piece will bring up a detailed Transactions Processed report for that transaction type. Right click on any of the charts to save that chart as a graphic in jpeg format. You can then import the graphic into your presentations or documents as needed.

- **Strip Chart**

  The Line Chart report shows the transaction totals by type in a line chart format. Each transaction type is shown in a different colour. Each coloured line represents the total amount of all transactions of that type. At the bottom of the chart, a table shows summary statistics for each type of transaction. Click on any of the legend boxes to see a line chart for that transaction type alone. Right click on any of the charts to save that chart as a graphic in jpeg format. You can then import the graphic into your presentations or documents as needed.

5.3 Orders Report
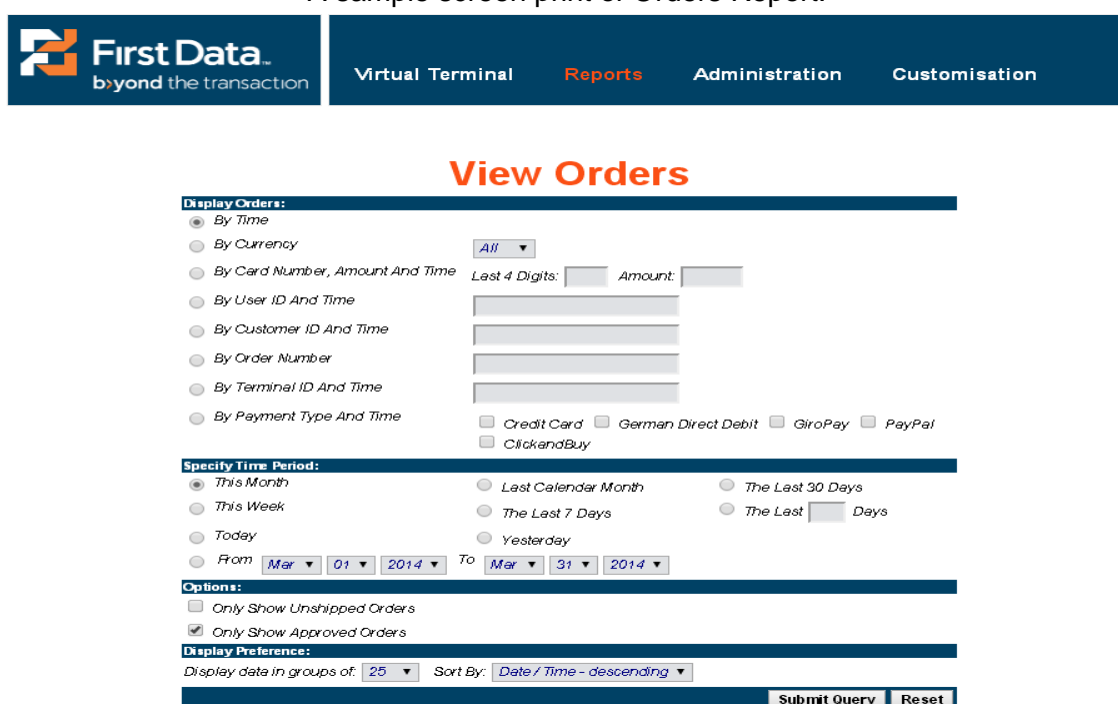
To view the Orders and generate an orders report follow these steps:

1. Click on the Reports button in the Main Menu Bar.
2. Click on the Orders link in the Side Menu Box. The View Orders screen appears.
3. **Display Orders**: select an option. You can view orders sorted by time period, by credit card number and time, by User ID and time, or by order number.
4. **Specify Time Period:** select any of the named time periods or enter a specific range of dates you wish to view.
5. **Options:** click on a box if you want the report to show only unshipped orders or to show only approved orders. By default, the *Only Show Unshipped Orders* box is unchecked and the *Only Show Approved Orders* box is checked, so the report will show approved orders only (both shipped and unshipped).
6. If the *Only Show Unshipped Orders* box is checked, the report will show all unshipped orders. If both boxes are unchecked, the report will display all orders (both shipped and

unshipped), including declined and recurring transactions with future start dates. If both boxes are checked, the report will show only all approved, unshipped orders.

7   **Display Preference:** this option allows you to choose how many orders will appear on each page of the report. Choose a number from the dropdown list.

8   **Select Hierarchy:** choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)

9   Click on the Submit Query button to view the report. If you want to re-enter the information, click on the Reset button to clear the information

A sample screen print of Orders Report:

The **Orders Received** report shows the following information about each order.

- **Select**—click on the associated Select checkbox to select one or more orders.
- **Shipped**—shows *Y* if the order has been shipped, or *N* if the order has not yet been marked as shipped.
- **Retail**—shows *Y* if the order was a retail order, or *N* if the order was not retail.
- **Order #**—the number associated with this order. Click on the order number to view order details.
- **User ID**—if there is a user ID number associated with the order, it will be listed in this column. The number is also a link to view all the orders placed by a particular customer.
- **Date**—the date that the order was placed. Shows the most recent order first. The time period you selected for the report will be shown under the report title.
- **Name**—the name of the person who placed the order. Click on the name to send email to this customer.
- **Authorised Amount**—The authorised amount of unshipped order (e.g. Pre-Auth).

- **Amount**—shows the amount and currency of the order. The total amount of the orders listed on the page and the total amount of all orders in this report is also shown at the bottom of the page, along with the total tax and shipping charges collected.

5.3.1 Confirming Shipment, Crediting Orders, Rejecting Orders

You can confirm shipment, credit the entire amount of the order(s), or reject order(s) by IP address or credit card number. To perform any of these three tasks, follow the steps below:

1   First select order(s) by clicking on the associated checkbox(es) in the left-most column.

2   Click on the *Work with Selected Orders* button. The Selected Order Menu screen appears.

3   Select an action by clicking on the appropriate radio button. If you select Reject Order, you must also check on a checkbox to choose whether you wish to reject this order by IP address or by credit card number. When you reject an order by IP address, all future orders from this IP address will be declined. When you reject an order by credit card number, all future orders using this credit card number will be declined.

4   Click on the Submit Query button to complete the task. A screen listing the results will appear.

If you choose to reject an order by IP address or credit card number, you will find yourself at the Fraud Settings page, which will show you all the IP addresses and credit card numbers you have currently blocked from purchasing at your store. The IP addresses or credit card numbers from the order(s) you just blocked should appear on this list.

To block more transactions or to un-block any IP address or credit card number, click on one of the links located towards the top of this screen, just under the title Your Fraud Settings. For more information on changing your fraud protection settings, see Preventing Fraud.

5.3.2 Order Details Report

To view this report, click on the Reports button on the Main Menu Bar, and then click on the Orders link in the Left Menu Box.

Select the appropriate parameters for your query, and then click the Submit Query button.

Once the Orders Report appears, you can view an order's detailed report by clicking on the associated Order # link.

The Order Detail Report allows you to:

- View the details associated with that order.
- E-mail the customer by clicking on the Name or E-mail link.
- Do a return (refund) against this order.
- View all the orders associated with the credit card number by clicking on the Card Number link.

The Order Detail report has several sections which show the following information:

- The Order ID Number and Order Date/Time are shown at the top of the report.
- Billing Address section—gives the User ID, shipping status, and the customer's company, name and address. If the customer's name and e-mail address were supplied, you can click on the customer's name to send an e-mail to the customer.
- Shipping Address section—shows the name, address to which the order was shipped.
- Contact Information section—shows the customer's telephone number, e-mail address, fax number and IP address. If an e-mail address was supplied, you can click on the customer's e-mail address to send an e-mail to the customer.
- The next part of the report includes subtotal, shipping, tax, return (if applicable) and total amounts.
- The last portion of the report is a General Information which shows the User ID, Order status (e.g. Has Shipped); IP Address; Transaction origin; Currency and the Cardholder Brand.
- The Return Order button allows you to do a return (initiate a refund) against this order. Enter the amount to refund to the customer in the box next to the Return Order button. The amount you enter must be equal to the total amount of the order. To process the return, click on the Return Order button. To return to the Reports Main Menu, click on the *Close Window* button.

5.4 Transactions Report

To view all your transactions, use the Transactions report. Follow the steps below:

1. Click on the *Reports* button on the Main Menu Bar.
2. Click on *Transactions* in the Side Menu Box.
3. In the *View Transactions* page —select an option. You can view transactions sorted by time period, by credit card number and time, by User ID and time, by transaction type and time, or by order number.
4. *Specify Time Period*—select any of the named time periods or enter a specific range of dates you wish to view.
5. *Select Hierarchy*: choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)
6. Submit Query—click to view the report.

To re-enter the information, click on the Reset button to clear the information.

The Transactions report shows the following information about each transaction. The time period you selected for the report will be shown just under the report title.

- **Order number**—shows the number associated with each order.
- **Date**—shows the date and time of each transaction, from the most recent order to the oldest order.
- **User ID**—if there is a user ID number associated with the order, it will be listed in this column. The number is also a link to view all the orders placed by a particular customer.
- **Type**—shows the type of transaction.
- **PayerAuth**—shows details about authentication (3D Secure)

- **Invoice Number #**—shows the Invoice ID that has been assigned when entering the transaction
- **PO #**— shows the Purchase Order that has been assigned when entering the transaction
- **Trans ID#**— shows the transaction id assigned by the Gateway to the transaction
- **Card/Account Number**—shows a link to view all transactions processed with that card or account number.
- **Exp. Date**—lists the expiry date of the card.
- **Approval**—shows the approval code of the transaction. If a specific transaction was declined, the reason it was declined is shown here.
- **Amount**—shows the amount and currency of the transaction

View the details of any order by clicking on the associated *Order #.*

View a list of all the numbers associated with any credit card number or routing number by clicking on the associated Card/Route Number.

If there are more transactions than will fit on the current page (according to the number of transactions you've chosen to show on each page), a set of numbers will appear at the bottom of the page, reflecting page numbers for the report. The current page number will be larger than the others and will not be underlined. To view any page, click on the associated underlined page number.

5.5 Transaction Summary Report

To view your entire transaction summary, follow the steps below:

1 Click on the *Reports* button on the Main Menu Bar.
2 Click on *Transaction Summary* in the Side Menu Box.
3 In the Transaction Summary page, select options. You can enter a specific User ID or select specific transaction types and/or card types to include in the report.
4 *Specify Time Period*—select any of the named time periods or enter a specific range of dates you wish to view.
5 *Display Preference*-choose the number of things you wish to display on one page by clicking on the dropdown box and selecting the number desired. The default is 25.
6 *Select Hierarchy*: choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)
7 Submit Query—click to view the report.

If you want to re-enter the information, click on the Reset button to clear the information.

Authorisation Summary Table:

The first table that appears in the Transactions Summary report shows the following summary information for each selected transaction type over the time period specified.

- **Approved**—shows the total number of approved transactions of that type and the total amount for all approved transactions of that type.
- **Declined**—shows the total number of declined transactions of that type and the total amount for all declined transactions of that type.
- **Total**—shows the total number of transactions of that type and the total amount for all transactions of that type.

The totals for each column are listed at the bottom of the table.

Approved Summary by Card Type Table:

The second table that appears in the Transactions Summary report shows the following summary information for each selected payment type over the time period specified.

- **#**—shows the total number of approved transactions for that payment type.
- **Amount**—shows the total amount for approved transactions of that payment type.
- **Total**—shows the total number of transactions of that type and the total amount for all transactions of that type.

The totals for each column are listed at the bottom of the table.

5.6 Credit Card Batches Report

To view all payment card batches processed. Follow the steps outlined below.

1   Click on the *Reports* button on the Main Menu Bar.
2   Click on *Credit Card Batches* in the Side Menu Box.
3   In the Credit Card Batches page, *Specify Time Period*—select any of the named time periods or enter a specific range of dates you wish to view.
4   *Display Preference*-choose the number of things you wish to display on one page by clicking on the dropdown box and selecting the number desired. The default is 25.
5   *Select Hierarchy*: choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)
6   Submit Query—click to view the report.

Credit Card Batches Table:

The first table that appears in the Credit Card Batches report shows the following summary information

- **Date**—shows the date and time of previous batches, from the most recent batch.
- **Count**—shows the total number of transactions in the batch.
- **Response**- Shows the response from the batch- This functionality is not currently available
- **Total**—shows the total amount processed.

Click on *Current Batch* hyperlink if you wish to view the batch yet to be processed by the Gateway.

The **Current Batch** report shows the following information about each order.

- **Select**—click on the associated Select checkbox to select one or more orders.
- **Order #**—the number associated with this order. Click on the order number to view order details.
- **Date**—the date that the order was placed.
- **User ID**—if there is a user ID number associated with the order, it will be listed in this column. The number is also a link to view all the orders placed by a particular customer.
- **Type**—the type of transaction (e.g. Sale).
- **Card/Route Number**- shows a link to view all transactions processed with that card or account number.
- **Exp. Dat*e***—lists the expiry date of the card.
- **Approval**—shows the approval code of the transaction.
- **Amount**—shows the amount and currency of the transaction
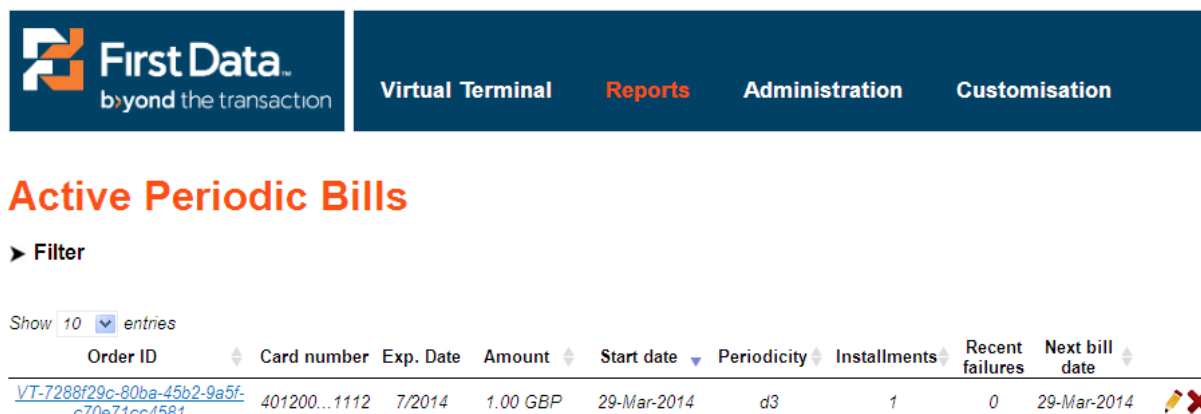
See section 4.8 on how to void transactions before the current batch is processed.

5.7 Active Periodic Bills (Recurring Transactions) Report

To view all your active periodic billing (Recurring Transactions), use the Active Periodic Bills report. Follow the steps outlined below to see this report.

1   Click on the *Reports* button on the Main Menu Bar.
2   Click on *Active Periodic Bills* in the Side Menu Box- the *Active Periodic Bills* page appears.

Sample screen print of Active Periodic Bills page:

The Active Periodic Bills report shows the following information about each recurring payment.

- **Order ID**—shows the Order ID associated with each recurring payment.
- **Card number**—shows the card number that will be charged
- **Exp. Date**—lists the expiry date of the card.
- **Amount**—shows the amount and currency of the transaction
- **Start date**—shows the start date of each recurring billing.
- **Periodicity**—shows the period the customer will be billed. Example, *d3* means the card will be charged every 3 days *w6* means the card will be charged every 6 weeks, *m1* means the card will be charged every 1 month etc.
- **Installments**—shows the number of times the card will be charged.
- **Recent Failures**—shows the number of times an attempt to charge the card failed. This resets to zero (0) once a transaction has been authorised on the card.
- **Next bill date**—shows the date the next date the card will be charged.

5.7.1 Modify Periodic Bill (Recurring Payment)

To modify an existing Recurring Payment, follow the steps outlined below:

1. Click on the *Reports* button on the Main Menu Bar.
2. Click on *Active Periodic Bill* in the Side Menu Box-the *Active Periodic Bills* page appears.
3. Click on Modify Periodic Bill (the pencil sign)- the *Modify Periodic Bill* page appears
4. Apply the changes you wish in the relevant text boxes
5. Click on Save Changes

5.7.2 Cancel Periodic Bill (Recurring Payment)

To cancel an existing Recurring Payment, follow the steps outlined below:

1   Click on the *Reports* button on the Main Menu Bar
2   Click on *Active Periodic Bill* in the Side Menu Box-the *Active Periodic Bills* page appears.
3   Click on Cancel Periodic Bill (the red cancel sign)
4   A message will pop for you to confirm cancelation
5   Click OK to confirm cancellation of the Recurring Billing.

Note: A Recurring Payment set to take daily will have a default decline/fail threshold of 3 consecutive days; a recurring payment set-up for monthly will have a default decline/fail threshold of 10 consecutive days and a recurring payment set for weekly will have a decline/fail threshold of 5 consecutive days.

What this means is that if an attempt decline/fail, the FDMS payment gateway will keep trying to take the payment until the threshold is reached then the cardholder's account will be deleted.

Please ensure you contact cardholder as soon as you notice a recurring payment failure/decline. It is highly recommended you set up a notification email for recurring payment (see section and sub sections 6.3)"

Contact the technical team (see section 1.2) if you would like to discuss the thresholds.

6 Virtual Terminal Administration

The Virtual Terminal Administration can be used to administer the store and its users.

To view the Administration tools, click on the Administration button on the Main Menu Bar.

The Administration Main Menu for your store is displayed in the Side Menu Box and in the main content portion of the screen. The tools available are listed below.

Manage users:

- **Change password**—You can change your password once successfully signed in.
- **Add/remove/modify user**—You to add new users to the store and administer permissions.

Fraud Settings:

- **Add/change card numbers to block**—You can block card numbers from here.
- **Add/change names to block**—You can add or change names of customers to block.
- **Add/change domain names to block**—You can or change domain names to block
- **Add/change IP/Class C addresses to block**—You can add or change IP addresses to block.
- **Set Maximum Purchase Amount**—You can set maximum purchase amount on your store.
- **Set lock out times**—You can set transaction lock out times.
- **Set country profile**—You can set countries you wish to accept transactions from
- **View your fraud settings**—You can view all your fraud settings in your store.

Transaction notifications settings:

- **Set options for transaction notifications via email**—You can set your email notifications here.
- **Set notification options for expiring customer data**—You can set email notifications for expiring stored card numbers in the Data Vault.

Screen print of Administration menu:
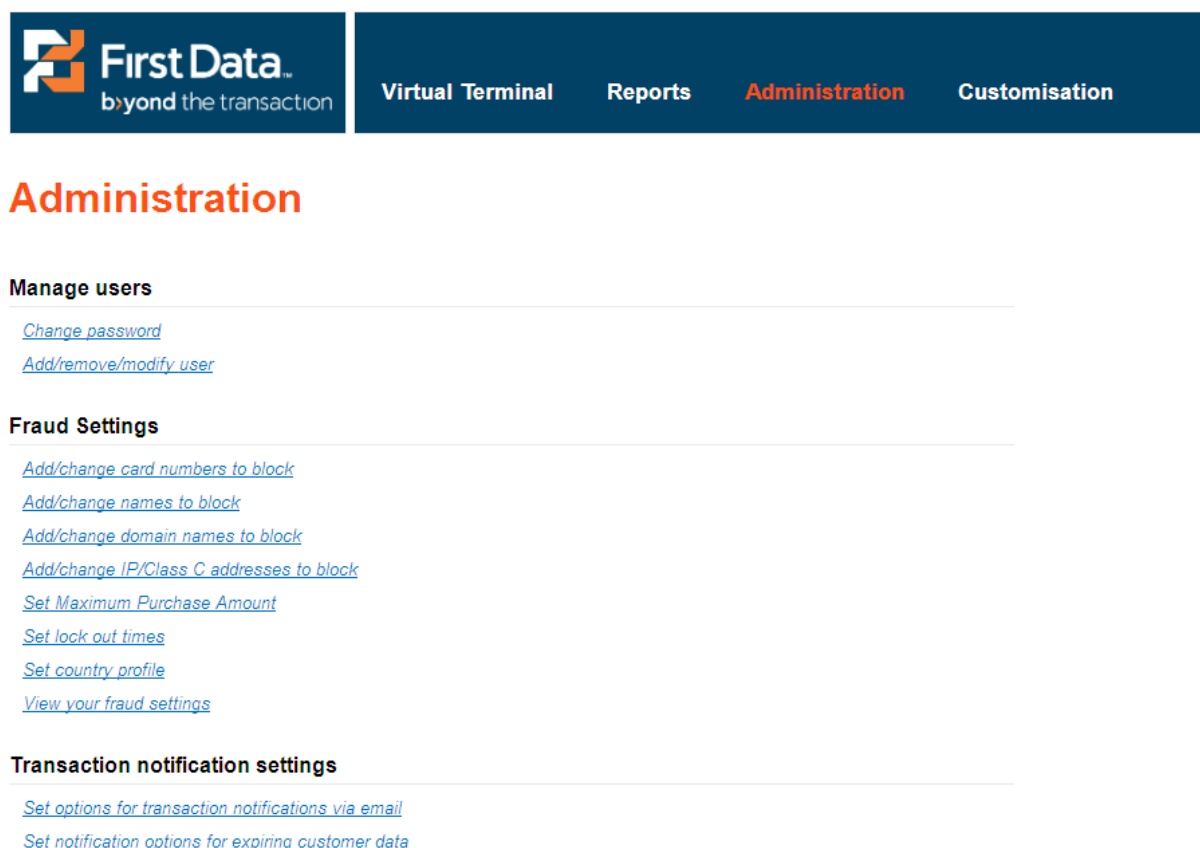
The following sub sections will describe how to access and utilise the above listed administration functions.

6.1 Manage Users

There are two functions under Manage Users which allows you to change password and add or remove or modify multiple users of your Virtual Terminal.
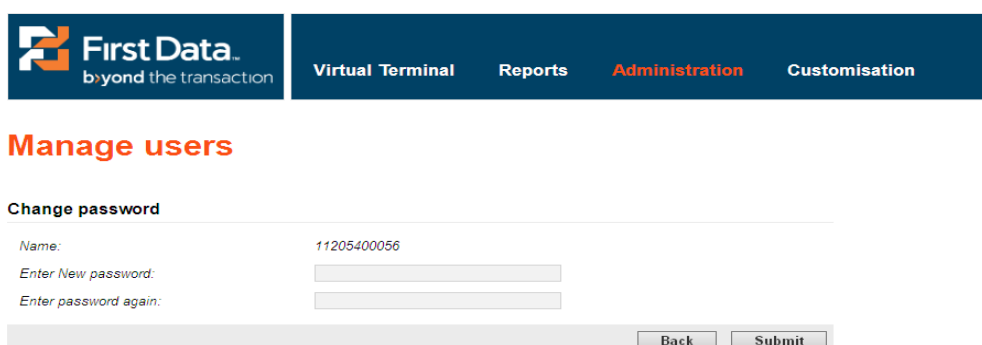
6.1.1 Change Password

When you first sign up for an account with the First Data Virtual Terminal, a temporary password shall be issued, the *Change Password* feature enable you to change the First Data issued password.

To change your password for the First Data Virtual Terminal, follow the steps below:

1   Select Administration on the Main Menu Bar

2   Click on '*Change Password'*- this will bring up the Change Password page.

3   Type your new password into the New password text box- Password must be minimum 7 alphanumeric and numeric characters (see notes below).

4   Re- enter password in the *Enter password again* text box

5   Click the *Submit* button

If the new password does not match an error will indicate, follow the steps above again.

Screen print of Change Password page:

Notes: FDMS highly recommended you avoid using common words or numbers as passwords - especially words or numbers that might be associated with you- e.g. name or your date of birth.

A simple approach will be to choose a memorable phrase - not a word. Put together the first letter from each word in the phrase, then the string of letters becomes your password. The phrase should consist of at least six words, to produce at least a six letter password. In addition, the password needs to have at least one numeric character.

6.1.2 Add/Remove/Modify User

The First Data Virtual Terminal enables multiple users for a single store, if you prefer different stores for different users (e.g. due to employee location and business requirements, contact First Data).

Multiple users of a single store can share the same Client Certificate.

To access the Virtual Terminal from a user's own device or machine, they will have to install the digital certificate on the respective machine(s) or device(s) -See Appendix A.

Add User(s)

To add users follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select Administration on the Main Menu Bar.

3   Click on *'Add/remove/modify user '*- this will bring up the *Manage users* page

4   Click on '*add*' link located at the bottom of page- this will bring up the *Add user* page

5 Complete the text boxes by entering a Username, a Password and confirm the password- password must be minimum 7 alphanumeric and numeric characters.

6 Click on *Continue*

7 The Current Users list will reappear, showing the new user on the list

Delete User(s)

To delete users follow the steps outlined below:

1 Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2 Select Administration on the Main Menu Bar.

3 Click on *'Add/remove/modify user'*- this will bring up the *Manage users* page with the Current Users list

4 Click on the delete link located next to the user you wish to delete.

5 A dialogue box will appear, stating that this operation will delete the selected user

6 Click the OK button to delete the user or Cancel if you do not wish to delete the

7   Once the user is deleted, the Current Users screen will refresh, with the deleted user omitted from the list.

Reset User(s) Password

To reset user(s) password follow the steps outlined below:

1 Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2 Select Administration on the Main Menu Bar.

3 Click on *'Add/remove/modify user'*- this will bring up the *Manage users* page with the Current Users list

4 Click on the *reset password* link for the appropriate user.

5 Enter New password for user

6 Enter password again

7 Click on *Submit* button

Note: The user can change their temporary password when they log in by using the *Change Password* function.

Setting User(s) Permissions

To set permission for users of your Virtual Terminal follow the steps outlined below:

1 Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2 Select Administration on the Main Menu Bar.

3 Click on *'Add/remove/modify user'*- this will bring up the *Manage users* page with the Current Users list

4   Click on the *permissions* link associated with the desired user- this will bring up the *Edit user permissions* page

5   In the Permissions portion of the table, click on the appropriate checkboxes to turn on or off permissions for this user.

6   You can control the user's following access:

  - View Reports
  - Process Transactions
  - Issue Credits.

7   Click on the *Continue* button at the bottom of the page

8   You will be returned to the Current Users listing. The words "updated successfully" should appear at the top of the page if the change was successful.

6.2 Fraud Settings (Fraud Prevention Tools)

There are several ways that the First Data Merchant Solutions Payment Gateway helps you prevent fraud from interfering with your business success. If certain individuals are continuously hurting your business with costly charge-backs, you can block them from purchasing at your store.

The tool has the capability to block card numbers, names, domain names, and IP or Class C addresses from purchasing at your store. In addition, two further capabilities are available, and these are the power to set a limit on the maximum purchase that can be made at your store, and the ability to set auto lockout and duplicate lockout times.

Fraud settings are sequentially ordered, so once you've finished with one, you can proceed to the next fraud setting. There is also a quick navigation bar at the right of each Fraud Setting page, which allows you to jump immediately to any Fraud Setting (See Section 6 of this guide for the full list).

Another way to prevent fraud is by paying close attention to the Address Verification response. If the address and/or post-code do not match the card-issuing bank's address on record, there is a higher probability of fraud (See Appendix B for a full description of the Address Verification response)

First Data highly recommend you use the Card Security Code field (See Section 4.1.1 of this guide).

The following sub sections describe how to use the fraud tools.

6.2.1 Blocking Card Number(s)

This section describes how to add card numbers for the system to block from processing orders and delete card numbers on the block card list.

Adding card number(s) to Block List:

To block any card number(s) you do not wish to allow to purchase at your store follow the steps outlined below:

1. Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).
2. Select Administration on the Main Menu Bar.
3. Click on *Add/change card numbers to block'*- this will bring up the *Block Card Numbers* page. If you have any card numbers already on your blocked credit cards list, they will automatically appear in the select box on the right side of the screen.
4. Enter the card number you wish to block in the *Card #* input text box on the left-hand side of the screen.
5. If you do not know the card number you can use the *Order Number* of the transaction where the card has been used instead.
6. Click on the *Add* button- the Payment Gateway will add the card number to the Store list of blocked card numbers, this will show on a drop down list at the right side of the page.

Add as many card numbers as you like by following steps 1-5 above.

Removing/Deleting Blocked card number(s):

To remove/delete a blocked card from your list, follow the steps outlined below:

1. Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).
2. Select *Administration* on the Main Menu Bar.
3. Click on *Add/change card numbers to block'*- this will bring up the *Block Card Numbers* page. If you have any card numbers already on your blocked credit cards list, they will automatically appear in the select box on the right side of the screen.
4. Select the card number in the select box on the right side of the screen and then click the *Delete* button.

Upon removal from your blocked card list, the card number will again be allowed to be used to purchase at your store. Delete as many card numbers as you need by repeating the same process.

Click on the *Next* button if you wish to go to the next fraud setting page.

If you wish to see all your fraud settings, click on the '*View All Fraud Settings'* button.

6.2.2 Blocking Name(s)

This section describes how to add names for the system to block from processing orders and delete names on the blocked list.

Caution must be taken in using this functionality as the name to be blocked MUST be exact much (i.e. character for character, space for space and case sensitive). Example, if you block the name "*John Redenbacher*" from your store, "*Johnny Redenbacher*", "*John Samuel Redenbacher*" or "*John S. Redenbacher*" would not be blocked.

Also, because the First Data Merchant Solutions Payment Gateway fraud system cannot distinguish between one "*John Smith*" and another, you will block all persons with the same name as the person you wish to block.

Adding name(s) to Block List:

To block particular names from purchase on your store follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Administration* on the Main Menu Bar.

3   Click on 'Add */ change names to block'*- this will bring up the *Block by Name* page. If you have any names already on your blocked name list, they will automatically appear in the select box on the right side of the screen.

4   Enter the name you wish to block in the *Name* input text box on the left-hand

     side of the screen. If you do not know the name of the customer you can use the *Order Number* of the transaction where the name has been used instead.

5   Click on the *Add* button- the Payment Gateway will add the name to the Store list of blocked names, this will show on a drop down list at the right side of the page.

Add as many names as you like by following steps 1-5 above.

Removing/Deleting Blocked name(s):

To remove/delete a blocked name from your list, follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Administration* on the Main Menu Bar.

3   Click on *'Add/change names to block'*- this will bring up the *Block by Name* page. If you have any names already on your blocked name list, they will automatically appear in the select box on the right side of the screen.

4   Select the name in the select box on the right side of the screen, then click the << Delete button.

Delete as many names as you like by following steps 1-4 above.

6.2.3 Blocking Domain Name(s)

This section describes how to add or delete domain names for individuals from domains that you do not wish to allow to purchase at your online store.

Adding Domain name(s) to Block List:

To block particular domain names from purchasing on your online store follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Administration* on the Main Menu Bar.

3   Click on *'Add / change domain names to block'-* this will bring up the *Block by Domain Name* page. If you have any names already on your blocked domain name list, they will automatically appear in the select box on the right side of the screen.

4   Enter the domain name in the Domain name input box on the left-hand side of the screen and then click the *Add* button. You must enter a domain in valid domain name format (e. g., *here.com*, *there.net*, *savetheworld.org*, *universityX.edu*)

5   Click on the *Add* button- the Payment Gateway will add the domain name to the Store list of blocked domain names, this will show on a drop down list at the right side of the page.

Add as many names as you like by following steps 1-5 above.

Removing/Deleting Blocked Domain name(s):

To remove/delete a blocked domain name from your list, follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select Administration on the Main Menu Bar.

3   Click on *'Add / Change domain names to block'-* this will bring up the *Block by Domain Name* page. If you have any names already on your blocked domain name list, they will automatically appear in the select box on the right side of the screen.

4   To remove a blocked domain from your list, select the domain name in the select box on the right side of the screen, then click the *Delete* button.

Delete as many domains as you need by following steps 1-4 above.

6.2.4 Blocking IP and Class C Addresses

This section describes how to add or delete Internet Protocol (IP) and Class C addresses for people or organisations that you do not wish to allow to purchase at your store.

Adding IP or Class C addresses to Block List:

To block particular IP or Class C address(es) from purchasing on your online store follow the steps outlined below:

1. Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2. Select Administration on the Main Menu Bar.

3. Click on *'Add / Change IP / Class C addresses to block'* - this will bring up the *Block IP/Class C Addresses* page. If you have any IP or Class C addresses already on your IP or Class C list, they will automatically appear in the select box on the right side of the screen.

4. Enter the address in the *IP/Class C* input box on the left-hand side of the screen.

5. You must enter IP addresses in the standard format, which is four numbers separated by 3 decimal points (e. g., 123.123.123.123).

6. To enter Class C addresses, enter the first 3 numbers separated by decimal points with a decimal point at the end (e. g., 123.123.123.)

7. If you do not know the address you can use the *Order Number* of the transaction where the IP/Class C address has been used instead.

8. Click the Add button- the Payment Gateway will add the IP/Class C address to the Store list of blocked IPs/Class Cs, this will show on a drop down list at the right side of the page.

Add as many IP or Class C addresses as you like by following steps 1-5 above.

Removing/Deleting Blocked Domain name(s):

To remove/delete a blocked IP/Class C from your list, follow the steps outlined below:

1. Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).
2. Select Administration on the Main Menu Bar.
3. Click on *'Add / change IP / Class C addresses to block'*- this will bring up the *Block IP / Class C Addresses* page. If you have any IP or Class C addresses already on your IP or Class C list, they will automatically appear in the select box on the right side of the screen.
4. To remove a blocked IP/Class C from your list, select the address in the select box on the right side of the screen, then click the *Delete* button.

Delete as many addresses as you need by following steps 1-4 above.

6.2.5 Setting Maximum Purchase Limit

This section describes how to set a maximum transaction amount that can be accepted on your store.

To set maximum purchase limit, follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Administration* on the Main Menu Bar.

3   Click on 'Set Maximum Purchase Amount'- this will bring up the Set Maximum Purchase Amount page.

4   Enter the maximum purchase amount next to the currency input box.

5   Click *Submit*

You can amend the amount by following steps 1-5 above.

6.2.6 Setting Auto Lockout time

This section describes how to set an automatic lockout time and duplicate lockout time.

To set lock out times, follow these steps:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select Administration on the Main Menu Bar.

3   Click on 'Set lock out times'- this will bring up the Set Auto Lock out Time and Set Duplicate Lock out Time.

- *Set lock out times*: Enables you to set how long an automatically blocked transaction will remain blocked.
- *Set Duplicate Lock out Time*: Enables you to set how long a duplicate transaction should remain blocked.
  That is, if two transactions are identical and they both occur within a length of time less than the specified duplicate lockout time, they will be automatically blocked as duplicate transactions.

4   Enter the time in seconds as per your business fraud rules in the *Auto Lock out Time* and/or *Set Duplicate Lock out Time* input boxes.

5   Click *Submit*

You can amend the time by following steps 1-5 above.

6.2.7 Setting Country Profile

This section describes how to set a Country Profile on your store to constrain card acceptance to cards from specific countries.

To set Country Profile, follow these steps:

1 Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2 Select *Administration* on the Main Menu Bar.

3 Click on *'Set country profile'* - this will bring up the *Set country profile* page.

4 Select one of the five profiles

- **Profile 1**: Your Store will only accept cards issued in the selected Country.
- **Profile 2**: Your Store will only accept cards issued from the listed 16 countries
- **Profile 3**: Your Store will only accept cards in the 16 countries in profile 2 and the additional 5 countries.
- **Profile 4**: Your Store will accept cards issued in all countries with the exception of the exception of 18 countries on the list.
- **Profile 5**: Your Store will accept cards from all countries.

5 Click *Submit*

You can amend the country profile by following steps 1-5 above.

6.2.8 View Your Store Fraud Setting

This section describes how to view a summary of all your store fraud setting.

To view your fraud setting, follow these steps:

1 Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2 Select Administration on the Main Menu Bar.

3 Click on *'View your fraud settings'* - this will bring up the *Fraud Settings* page.

4 If you wish to amend any setting click on *Change Settings* button and follow the steps outlined in this Guide.

6.3 Transaction Notifications

The First Data Merchant Solutions Payment Gateway can be configured to automatically send out confirmations for each payment transaction by email. These notifications can be sent to you as well as to your customer.

6.3.1 Transaction Notification by Email

To set Transaction Notifications via email, follow these steps:

5   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

6   Select Administration on the Main Menu Bar.

7   Click on 'Set options for transaction notifications via email'- this will bring up the Notifications page.

8   Select Enable Notifications.

9   In Address settings:

- Enter your email address for receiving transaction notifications in the first input box and select your preferred language for notifications.
- Enter your email address for sending notifications to your customer(s) in the second input box.
- Enter your company/store name to be displayed in email to your customer(s)

10   Click on the *Save Changes* button at the bottom of the page.

Individual text for email to customer

If you wish to insert additional text for the notifications to your customer, follow these steps:

1   After you have enabled notifications (see section 6.3.1), click on View/modify individual text to be displayed in the email to your customer.

2   The *Individual text for email to customer* page will appear, apply the text to the two available input boxes.

3   Click on the Preview email to check the format.

4   Click *Save Changes* button if you are happy with the format.

Notification Events

If you wish to configure events when email notifications should be sent to you and/or your customer, follow these steps:

1   After you have enabled notifications (see section 6.3.1), click on View/configure the events where you want to send/receive a notification

2   The *Transaction notifications via email* page will appear with a list of transactions supported on the Gateway.

3   Select the events you would like to receive notification email- e.g. if transaction Approved or Decline.

4   Click *Save Changes* button.

6.3.2 Email Notification-Expiring Data Vault details

This facility can only be used if you have stored cardholder details using the First Data Payment Gateway Data Vault via your online store (FDMS EMEA Connect or FDMS EMEA Web Service API).

To set up Email Notifications for expiring stored card details, follow the steps outlined below:

1. Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2. Select Administration on the Main Menu Bar.

3. Click on 'Set notification options for expiring customer data'- this will bring up the Notifications page.

4. Enter the email address where you would like the notification to be sent to in the *Contact Email* text box.

5. Tick the 'Activate email notifications for expiring customer data' check box.

6. Input the number of months in advance you would like to be notified in the '*Number of months in advance*' text box.

7. Select the language for email.

8. Click on the *Submit* button.

7 Virtual Terminal Customisation

The Virtual Terminal Customisation can be used to customise your website (online shop) and the Virtual Terminal.

To view the customisastion tools, click on the Customisation button on the Main Menu Bar.

The Customisation Main Menu for your store is displayed in the Side Menu Box and in the main content portion of the screen. The tools available are listed below.
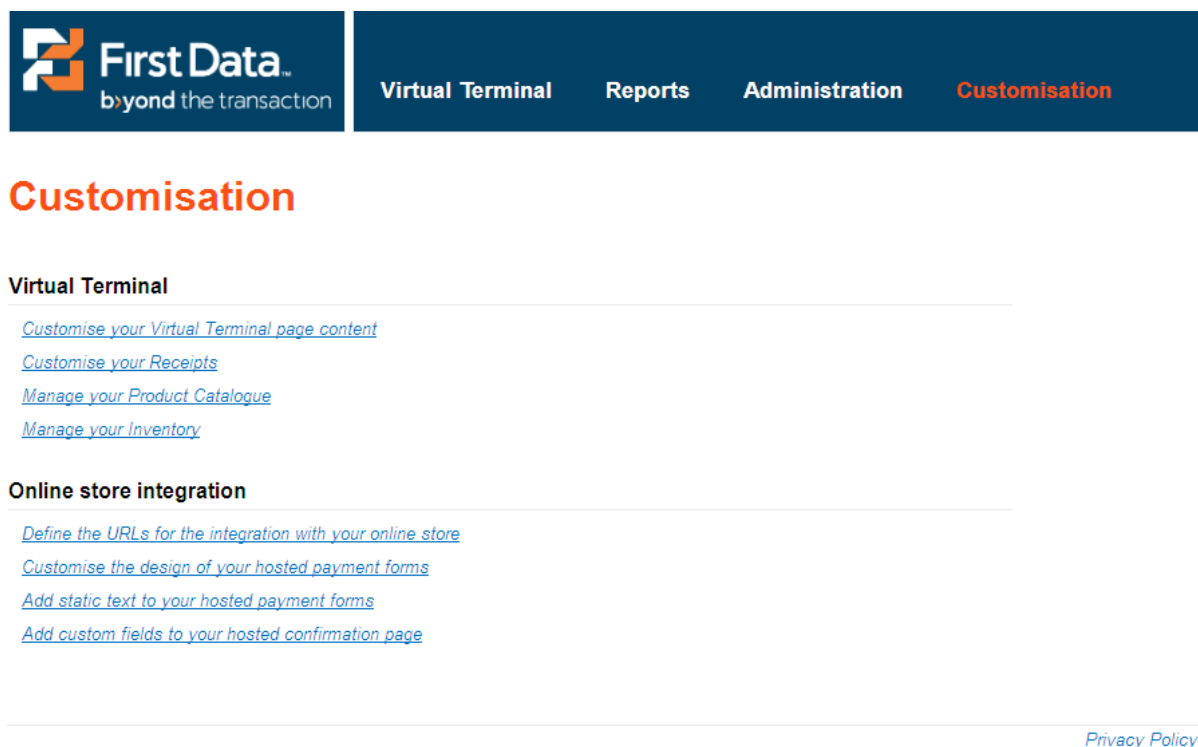
Virtual Terminal:

- **Customise your Virtual Terminal page content**—You can customise the Virtual Terminal Point of Sale form content here.
- **Customise your Receipts**—You can customise your transaction receipts here.
- **Manage your Product Catalogue** —You can add or delete items from your Product Catalogue here.
- **Manage your Inventory** —You can update your inventory information for your products here.

Online Store Integration:

- **Define the URLs for the integration with your online store** —You can set your website success or failed transaction URL, including transaction notifications.
- **Customise the design of your hosted payment forms** —You can design the First Data Connect hosted payment page here.
- **Add static text to your hosted payment forms** —You can add your own text to be displayed on the First Data Connect hosted payment page here.
- **Add custom fields to your hosted confirmation page** —You can set countries you wish to accept transactions from
- **View your fraud settings**—You can add your own custom field to display in the confirmation field here.

Screen print of Customisation menu:

7.1 Customising Your Virtual Terminal Page Content

To customise your Virtual Terminal page content in order to meet your business needs follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Customisation* on the Main Menu Bar.

3   Click on 'Customise your Virtual Terminal page content'- this will bring up the POS Custom Form Content page.

4   Un-tick the *Visible* check box for any field which you do not want to appear at the Point of Sale.

5   Tick *Required* check box for any field which you want all Virtual Terminal users to input as part of the order process (e.g. Invoice Number, Email address can be made mandatory).

6   Select Default items for Currency, Transaction Origin or Transaction Type as per your business requirement. First Data strongly recommends MOTO is made default for Transaction Origin field.

7   Click *Submit*

You can amend/reverse the customisation of the Virtual Terminal page content by following steps 1-7 above.

To restore the default settings, click on the '*Get Defaults'* button at the bottom of the page, then click on the 'Submit' button.

Note: Some of the fields cannot be removed from the page; if this is the case, they either do not appear in the listing, or they may appear in the listing with a checked graphic in front of them, rather than a checkbox which you can check or uncheck.

You might notice that not all the input fields appear on this page. Some fields are always required to process a transaction (for example, the card number is always required for a card purchase). Since these fields must always appear on your entry pages and they are always required, they are not customisable.

There are a few fields which cannot be made required: all fields related to Items and Recurring Payments. The Total Amount of the order is always required, so you are not allowed to change this either.

7.2 Customising Your Receipts

To customise your transaction receipts, follow the steps outlined below:

1 Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2 Select *Customisation* on the Main Menu Bar.

3 Click on *'Customise your Receipts'*- this will bring up the *Receipt* page.

4 Enter up to 24 characters in the Receipt Header textbox. This text will appear towards the top of your receipt.

5 Enter up to 24 characters in the Receipt Footer textbox. This text will appear at the bottom of your receipt.

6 Click on the 'Submit' button.

You can edit the customised receipt by following steps 1-6 above.

7.3 Managing Your Product Catalogue

The First Data Virtual Terminal offers you the time-saving ability to choose items from your own Product Catalogue every time you process an order.

7.3.1 Setting up a Product Catalogue

To set up a Product Catalogue in your Virtual Terminal, follow the steps outlined below:

1 Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2 Select *Customisation* on the Main Menu Bar.

3 Click on *'Manage your Product Catalogue'*- this will bring up the Product Catalogue page.

4 Add

- 'Product ID'

- 'Description',
- 'Price'
- 'Currency'

Click on *Add* this will bring up product settings page to customise the product, you have the option to edit products entered by clicking on '*Edit*' to add options (e.g. colour of product, size of product, make, brand etc.).

5   Click on *Submit* button

Follow steps 1 to 5 above for any new items you wish to add or amend in the catalogue.

7.3.2   Selecting Product from Product Catalogue

Upon setting up your Product Catalogue (see Section 7.3.1), you can process payments from the catalogue by following the steps outlined below:

1   Go to Point of Sale (by clicking on Virtual Terminal on the top menu)

2   Click on '*Select Products*' (this option will be available if you followed the steps described in section 7.3.1)

3   Enter the number of items in field '*Qty*' of the product you wish to select.

4   Click on '*Add Items(s)*', once Product(s) has been successfully added.

5   Click on 'POS Main'.

6   The correct quantity, choices, product description, price, and total should appear in the Selected Products table on the bottom half of the page.

7   Follow steps in section 4.1 if you wish to perform a Sale transaction.

Note: The top half of the page is the Product Summary table, which lists all the products in your product catalogue.

If there are any options for a selected product, they will appear in the Options column of Product Summary table- you can select the appropriate choice of option by choosing one of the options available in the drop down menu.

7.3.3 Deleting Selected Item(s) from Order

To delete selected items (as per section 7.3.2) following the steps outlined below:

1   Go to Point of Sale (by clicking on Virtual Terminal on the top menu)

2   Click on '*Select Products*' (this option will be available if you followed the steps described in section 7.3.1)

3   In the *Product Catalogue* page that appears (after step 2 above), scroll down to '*Selected Products*' table.

4   Click on the checkbox of the item you wish to delete or amend.

5   Click on 'Delete Items(s)'.

6   Follow the steps outline in section 7.3.2 if you wish to select a new item from the Product Catalogue.

Screen print of selected item from a Product Catalogue at POS:

Point of Sale

Required fields *Optional fields*

▼ Product Catalogue

| Select Products | | | | | | |

#	Qty	Item Id	Description	Options	Unit Cost	Extended Cost
1	1	Phone	Sim Free	Colour: Black	80.00 GBP	80.00 GBP
2	1	Tablet	iOS 7	Memory Size: 16 Gig	399.00 GBP	399.00 GBP
					Subtotal:	479.00 GBP

▼ Order Information

Order Number:	
Purchase Order Number:	
Invoice Number:	
Subtotal:	479.00
Delivery Amount:	
VAT (For International Orders):	
Total Amount:	479.00
Currency:	GBP

▼ Card   Credit Card

7.4 Managing Your Inventory

The First Data Virtual Terminal offers you an inventory management tool for your Product Catalogue (See Section and subsections 7.3 on how to set up a Product Catalogue).
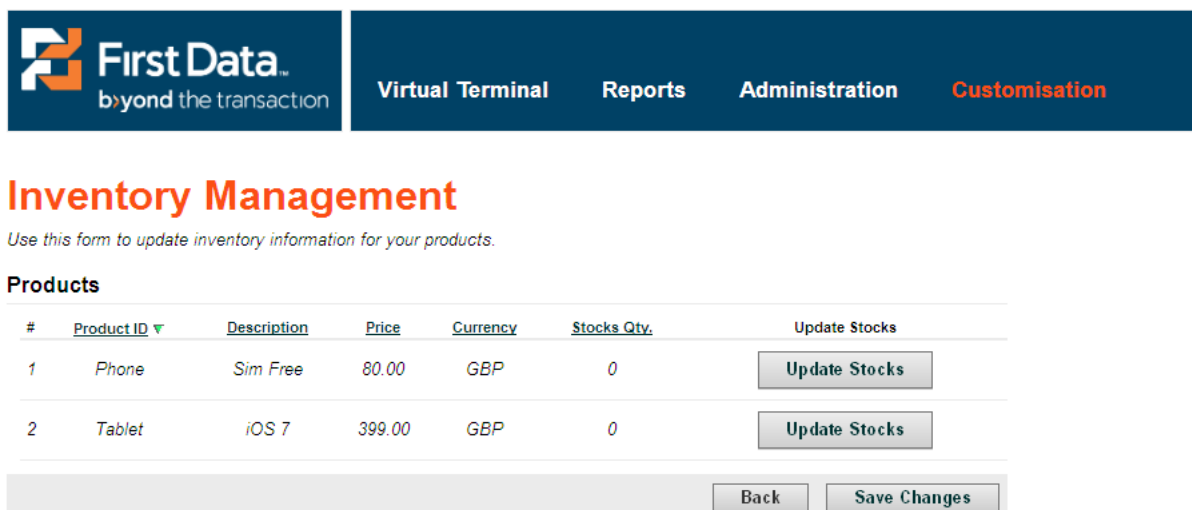
To manage your inventory in your Virtual Terminal, follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Customisation* on the Main Menu Bar.

3   Click on *'Manage your Inventory'*- this will bring up the *Inventory Management* page. This will show all the products in your Virtual Terminal Product Catalogue and an *Update Stocks* button at the right hand column of the page for each product.

4   Click on *Update Stocks* of the product/item you wish to update-this will bring up details of the product and an input box.

5   Enter the number/quantity of stocks in the Update Stocks input box.

6   Click *Save Changes* to update the inventory information for the product.

Follow steps 1 to 6 above to update any additional inventory information for your products in the Virtual Terminal.

Note: To delete an item in your Product Catalogue, you will have to reset stocks for that item in Inventory Management.

Screen print of Inventory Management page:

Inventory Management

Use this form to update inventory information for your products.

Products

#	Product ID ▼	Description	Price	Currency	Stocks Qty.	Update Stocks
1	Phone	Sim Free	80.00	GBP	0	Update Stocks
2	Tablet	iOS 7	399.00	GBP	0	Update Stocks

Back   Save Changes

Privacy Policy

7.5 Settings for your FDMS Connect Payment Gateway

The information contained in this and subsequent sections are applicable only if you are using the FDMS EMEA Connect Payment Gateway.

Please consult with your web developer before using any of the functions outlined in this section as misuse can impact customers at your website.

7.5.1 Define your FDMS EMEA Connect Payment Gateway URL

To define the FDMS EMEA Connect URLs in your Virtual Terminal, follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Customisation* on the Main Menu Bar.

3   Click on 'Define the URLs for the integration with your online store'- this will bring up the Online store URL settings page.

4   See detailed explanation of the following in this guide:

- Confirmation Page ("Thank You")
- Failure Page ("Sorry")
- Transaction Notification (URL to receive notification when a transaction is complete)
- Overwrite Store URLs

5   Click on Submit button.

Follow steps 1 to 5 above if you wish to amend the URLs provided.

Confirmation Page ("Thank You")

This is where you tell the FDMS Payment Gateway where to redirect customers after a successful transaction.

1   If you leave the *URL (text only)* text box blank, then the Gateway will look for this URL in your Connect request message (parameter '*responseSuccessURL*'; please refer to the FDMS EMEA Connect Guide on how to implement this option).

2   If you un-tick the check box (*Automatically display specified URL after the payment process*), then the Gateway will display the default First Data Merchant Solutions confirmation page.

3   If you tick the check box (*Automatically display specified URL after the payment process*), then the Gateway will not display the default First Data Merchant Solutions confirmation page.

Screen print of default First Data Merchant Solutions confirmation/receipt page:

Failure Page URL

You may want to redirect customers whose transactions has been declined or failed to a specific page on your web site where they will find information on how to get in contact with you by e-mail or by phone to arrange alternative payment

This is where you tell the FDMS Payment Gateway where to redirect customers after a declined or failed transaction.

1 If you leave the *URL (text only)* text box blank, then the Gateway will look for this URL in your Connect request message (parameter '*responseFailureURL*'; please refer to the FDMS EMEA Connect Guide on how to implement this option).

2 If you un-tick the check box (*Automatically display specified URL after the payment process*), then the Gateway will display the default First Data Merchant Solutions failure/decline page; the URL you provided will be automatically displayed.

3 If you tick the check box (*Automatically display specified URL after the payment process*), then the Gateway will not display the default First Data Merchant Solutions failure/decline page; the URL you provided will be automatically displayed.

Screen print of default First Data Merchant Solutions failure page:

Transaction Notification URL

If you want the Payment Gateway to send you all the results of the payment transaction, you can use the transaction notification URL option to achieve this.

This is where you tell the FDMS Payment Gateway where to notify you of the results of the transaction.

1   If you leave the *URL (text only)* text box blank, then the Gateway will use the URL in your Connect request message (parameter '*transactionNotificationURL*'; please refer to the FDMS EMEA Connect Guide on how to implement this option).

2   If no URL are provided no result notification will be sent.

Overwrite Store URLs

If you want to be able to overwrite the URLs provided on the Online store URL settings in the Virtual Terminal (i.e. Confirmation Page, Failure Page, Transaction Notification) with the URL that will be sent in your online request as per the FDMS EMEA Connect Payment Gateway specification, then tick the check box '*Allow URLs to be overwritten by those in the request of Connect transaction*'.

7.5.2 Customise your FDMS EMEA Connect Hosted Page

To customise the design of your FDMS EMEA Connect hosted payment forms to align with your shop or corporate design, follow the steps outlined below:

1 Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2 Select *Customisation* on the Main Menu Bar.

3 Click on 'Customise the design of your hosted payment forms'- this will bring up the Design adjustments for hosted payment forms page.

4 Choose the Connect Pages link from the Customisation section to individually define the following elements, expand the element you wish to modify:

- **Background-Colours:** You can change the colour of the Header Area, Content and Footer Area of the hosted page from here.
- **Mobile:** You can change the colour of the Header Area if you are using the mobile pay flow (parameter '*mobileMode=true*') of the Connect payment page.
- **Amount Title:** You can adjust the Font type, size, colour and weight of the Amount title of the hosted page here.
- **Superscription:** You can adjust the Font type, size, colour and weight of the hosted page superscription.
- **Individual Text:** You can adjust the Font type, size, colour and weight of individual text on the hosted page.
- **Label:** You can adjust the Font type, size, colour and weight of labels on the on the hosted page.
- **Normal Text:** You can adjust the Font type, size, colour and weight of labels for normal text.
- **Buttons:** You can adjust the Font type, size, colour and weight of the hosted page buttons.
- **Anchor:** You can adjust the Font type, size, colour, background colour and weight of any hyperlink on the hosted page.
- **System Messages:** You can adjust the Font type, size, colour and weight for system messages.

5 Click '*Preview Style*' to review the design changes you have applied or *Mobile Preview Style* for the mobile page flow

6 Click '*Save Style'* if you are happy with the changes.

Follow steps 1 to 6 above if you wish to re-adjust the hosted payment forms.

Note: *Restore Reseller Default Setting* will restore the default FDMS Hosted Page settings.

7.5.3 Add Static Text to your FDMS Connect Payment Hosted Page

The default static text displayed on the FDMS page will be "All payment information is encrypted and transmitted only via a secure 128bit SSL (Secure Socket layer) connection."

If you wish to overwrite this, you can use the *adding static text* function in the Virtual Terminal.

Your text will then be shown to the cardholder on the right side of the payment page.

To add static text to your FDMS Hosted Page, follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Customisation* on the Main Menu Bar.

3   Click on 'Add static text to your hosted payment forms'- this will bring up the Customise text for the hosted payment forms page.

4   Update the text in the input box of your preferred language, check the alignment.

5   Click Submit button to update changes.

Follow steps 1 to 5 above if you wish to edit the static text.

Note: *Restore Reseller Default value* button will restore the default FDMS Hosted Page text.

If you would like to add your individual company logo on these pages, please contact the technical support team (See section 1.2 of this Guide).

7.5.4 Add Custom Fields to your FDMS Connect Payment Confirmation Page

To add a custom field to your hosted confirmation page, follow the steps outlined below:

1   Login to the Virtual Terminal with the Store ID and password (this will be the Store ID and password that was provided to the primary user of the Account. If password has been changed by the primary user, then use the Store ID and the new password).

2   Select *Customisation* on the Main Menu Bar.

3   Click on "Add custom fields to your hosted confirmation page"- this will bring up the Custom Fields page.

4   Tick the Viewable checkbox if you want customers to see the custom field, provide a name for the field in the Name textbox and then provide a caption for the custom field in the Caption text box.

5   Click the Add field button to add the custom field. You can add as many custom fields as you wish.

6   Click Submit button

Follow steps 1 to 6 above if you wish to add additional field. If you would like to delete a custom field from the confirmation page, click the Delete link at the Actions column of the field you would like to delete.

APPENDIX A: P12 Digital Certificate Installation

This part of Appendix A describes how to install p12 certificate in your browser, the Virtual Terminal works with all the major browsers.

A1. PC Windows IE and Google Chrome

To access the First Data Virtual Terminal via Internet Explorer or Chrome, you will require your Store Number and User ID log on details along with your Virtual Terminal Password and Certificate Password. Once you have this information, follow the steps outlined below:

- Double click on the file containing the .p12 certificate can be found attached to the email (e.g. *1120541234.p12)*.
- Certificate Import Wizard will appear Click *Next*
- The next Certificate Import Wizard dialogue box will state **File to Import** *Specify the file you want to import -* Click Next
- The next Certificate Import Wizard dialogue box will state **Password** *Type the password for the private key*.
- Enter the Certificate password which was provided to you by First Data:
- Leave the two check boxes un-ticked:

    - Enable strong key protection. You will be prompted every time the private key is used by an application you enable this option
    - Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

- Click Next the next Certificate Import Wizard dialogue box will state **Certificate Store.** Tick (if not already ticked) Automatically select the certificate store based on the type of certificate
- Click Next, the next Certificate Import Wizard dialogue box will state ***Completing the Certificate Import Wizard***
- Click Finish- you should see *The import was successful dialogue* box, click finish.
- Click on the First Data Virtual Terminal Interface URL that would have been provided to you in an email to access the Virtual terminal.
- You will be prompted to choose a digital certificate when login to the URL, select your store certificate and click OK.
- You should now be at the Merchant Login page.

A2. PC Mozilla Firefox

To access the First Data Virtual Terminal via Mozilla Firefox, you will require your Store Number and User ID log on details along with your Virtual Terminal Password and Certificate Password. Once you have this information, follow the steps outlined below:

- File containing the .p12 certificate can be found attached to the email (e.g. *1120541234.p12)*. Save the p12 digital certificate in a folder or your desktop.
- Open Mozilla Firefox and click on *Tools* in the top menu bar
- Scroll down to Options and click- Options dialogue box appears.
- Click on *Advanced* in the top menu bar
- Click on *Certificates-* the certificates options appear.
- Click on View Certificates- Certificate Manager dialogue box appears.
- Click on Your Certificates in the top menu bar.
- Click on *Import* button at the bottom of the Certificate Manager Dialogue box.
- Navigate to the folder or desktop where you saved your store certificate as per step one above.
- Double-click on the digital certificate- a Password Entry Dialogue box will appear.
- Enter the Certificate password which was provided to you by First Data
- If the password match an Alert dialogue box will appear- Successfully restored your security certificate(s) and private key(s)
- Click OK
- Click on the First Data Virtual Terminal Interface URL that would have been provided to you in an email to access the Virtual terminal or copy and paste the URL in your Mozilla Firefox if Firefox is not your default browser
- You will be prompted to choose a digital certificate when login to the URL, select your store certificate and click OK.
- You should now be at the Merchant Login page.

A3. MAC OS X

To access the First Data Virtual Terminal for MAC OS X, you will require your Store Number and User ID log on details along with your Virtual Terminal Password and Certificate Password. Once you have this information, follow the steps outlined below:

- File containing the .p12 certificate can be found attached to the email (e.g. *1120541234.p12)*. Download the p12 digital certificate.
- Double-click will bring the dialogue box ***Add Certificate*** "Do you want to add the certificate(s) from the file "1120541234.p12" to a keychain?"
- Click on *Add* button at the bottom of the Add Certificate box- The next dialogue box will prompt for a certificate password.
- Enter the Certificate password which was provided to you by First Data and click on OK button.
- Click on the First Data Virtual Terminal Interface URL or copy and paste in your Safari browser URL.
- You will be prompted to select certificate and click continue.
- You may get a dialogue box "com.apple.******" wants to sign using key "privateKey" in your keychain.
- Select "Always Allow".
- You should now be at the Merchant Login page.

Note: if you wish to access the Virtual Terminal via **Mozilla Firefox** on MAC follow the steps in Appendix A2 in this Guide, you will have to go through *Firefox* on the main menu bar->*Preferences->Advanced->Encryption->View Certificates->Your Certificates*

A3. iOS Safari

To access the First Data Virtual Terminal on an iOS, you will require your Store Number and User ID log on details along with your Virtual Terminal Password and Certificate Password. Once you have this information, follow the steps outlined below:

- File containing the .p12 certificate can be found attached to the email (e.g. *1120541234.p12)*. Click on the p12 digital certificate.
- Next phase will be Install Profile- Identify Certificate
- Click Install- a dialogue box will pop up- "Unsigned Profile" "Installing this profile will change settings on your device"
- Click Install Now.
- The next dialogue box will prompt for you device pass code- enter your device four digit passcode (this is the passcode you would normally use to unlock your device).
- Enter the Certificate password which was provided to you by First Data and click Next.
- Profile Installed- Click Done.
- Click on the First Data Virtual Terminal Interface URL or copy and paste in your Safari browser URL.
- You should now be at the Merchant Login page.

APPENDIX B: Approval Code Description

An example Approval Code for a successful transaction will look like this:

Y:356887:0000144820:PPXM:0612789753. Below table explains the values.

Value	Meaning
Y	Successful
356887	Issuer's approval code or processor reference number
0000144820	Payment Gateway Internal ID
PPXM	First three characters (**PPX**) indicate Address Verification Service Results: <table><tr><th>Value</th><th>Meaning</th></tr><tr><td>PPX</td><td>No address data provided or Address not checked by the Card Issuer.</td></tr><tr><td>YYY</td><td>Card Issuer confirmed that street and postcode match with their records.</td></tr><tr><td>YNA</td><td>Card Issuer confirmed that street matches with their records but postcode does not match.</td></tr><tr><td>NYZ</td><td>Card Issuer confirmed that postcode matches with their records but street does not match.</td></tr><tr><td>NNN</td><td>Both street and postcode do not match with the Card Issuer's records</td></tr><tr><td>YPX</td><td>Card Issuer confirmed that street matches with their records. The Issuer did not check the postcode.</td></tr><tr><td>PYX</td><td>Card Issuer confirmed that postcode matches with their records. The Issuer did not check the street.</td></tr><tr><td>XXU</td><td>Card Issuer did not check the AVS information</td></tr></table> The last alphabetic character in the middle (**M**) is a code indicating

whether the card security code matched the card-issuing bank's code. An "M" indicates that the code matched.

This code may or may not be present, depending on whether the card security code was passed and the service was available for the type of card used. Below is a table showing all the possible return codes and their meanings.

Value	Meaning
M	Card Security Code Match
N	Card Security Code does not match
P	Not processed
S	Merchant has indicated that the card security code is not present on the card
U	Issuer is not certified and/or has not provided encryption keys
X	No response from the credit card association was received
	A blank response should indicate that no code was sent and that there was no indication that the code was not present on the card.

0612789753	Payment Gateway Internal ID

An example decline or failed transaction will look like this: *N:54: EXPIRED CARD*

END OF DOCUMENT