PlugNPay WebXPress External Redirect Interface for Credit Card Processing

November 30, 2018

Copyright Information

Vermont Systems, Inc.
12 Market Place
Essex Junction, VT 05452
www.vermontsystems.com

Contents

PAGE LEFT BLANK FOR DOUBLE-SIDED PRINTING

PlugNPay WebXPress Overview

The PlugNPay WebXPress External Redirect IP Interface gateway provides results similar to the direct IP interfaces with the exception of entering any credit card information directly into RecTrac.

Note: The key to all External Redirect Interface (ERI) options is that no card data is entered, transmitted, or stored within a VSI application. This eliminates the need for extensive PA-DSS requirements.

This web based redirect option allows credit cards to be swiped on a magnetic stripe reader or manually entered by your staff into RecTrac and GolfTrac, or manually keyed on a web portal by your customers in WebTrac. This option stores no card data other than the card mask (first 6 & last 4 digits) in the VSI database and no card entry is performed on the screen of a VSI application. Clerks can use their existing keyboard wedge card readers; whereas WebTrac customers will continue to manually enter their card data on a new payment screen.

Important Notes!: If you use RecTrac and WebTrac, as well as utilize the Installment Billing/Auto-Debit feature within the software, it is **strongly advised** that you setup at least one separate account for each function with PlugNPay.

For example, if your organization uses all of these functions – RecTrac, WebTrac and Installment Billing/Auto-Debit – it would be recommended that you setup a minimum of three accounts with PlugNPay: an account for Retail transactions, an account for e-Commerce transactions, and another account for MOTO transactions (Installment Billing/Auto-Debit).

While it is not *required*, it is considered good practice by VSI to setup your accounts in this fashion. PlugNPay has the ability to process MOTO type transactions (Installment Billing/Auto-Debit) regardless of the account type; however, not every merchant will allow it. By setting up separate accounts for each function, this will ensure that transactions are processed consistently. **Please note that choosing to combine your merchant accounts may result in processing issues later, should your merchant's regulations change**.

License – Maintenance Agreement

The use of this interface requires a VSI license and annual maintenance agreement. Prior to implementing any process outlined in this document, please contact the Vermont Systems Sales department at 1-877-883-8757 to verify that you are authorized to use this interface or to obtain a quote and approval.

Workstation Minimum Requirements

In order to process credit card transactions using PlugNPay WebXPress, the workstations on which you process transactions (including your WebTrac Transaction server, if applicable) must meet the following requirements:

As of Sunday, July 11th, 2010 there will be a change made to the IP addresses for PlugNPay payment servers. Therefore, to continue processing credit cards without interruption, be sure to verify access to the following URL from each workstation:

- Be running RecTrac/GolfTrac/TeleTrac/WebTrac/PayTrac version 10.1r (or later) or 10.2h (or later)
- For restaurant/bar tip processing, you must be running RecTrac/GolfTrac/TeleTrac/WebTrac/PayTrac version 10.1r (or later) or 10.2h (or later).
- In order to run the ERI CC Conversion Mask Utility, you must be running RecTrac/GolfTrac/TeleTrac/WebTrac/PayTrac version 10.2k (or later).
- Have Microsoft Internet Explorer, version 5.0 or higher installed.

> **Note:** The RecTrac/GolfTrac/TeleTrac/WebTrac/PayTrac versions listed above are *minimum* requirements only. For best processing practice, VSI recommends keeping your database up to date with the most recent version whenever it becomes available. This information can be found on the home page of the VSI Website: www.vermontsystems.com.

Limitations

- You may NOT process debit cards UNLESS the card can also be used as a major credit card.
- You may not process restaurant type transactions which include tip processing UNLESS you are running RecTrac/GolfTrac/TeleTrac/WebTrac/PayTrac version 10.1r (or later).

- You may not process blind credits or sales via the RecTrac Credit Card Terminal program. Blind transactions can only be processed via the PlugNPay website. Processing blind transactions is discussed later in this document.
- Having installment billing periods of six months or more (billing semi-annually, annually, etc…) is not recommended. PlugNPay stores unique identifiers for approximately six months. If you bill semi-annually or annually, you run the risk of not having unique identifiers for your households and billing for those households will fail. VSI recommends no more than quarterly installment billing (quarterly, monthly, semi-monthly, bi-weekly, weekly).
- If you use Installment Billing with CC Auto-Debit and/or WebTrac E-Commerce, you ***cannot*** use the Duplicate Check feature on the PlugNPay account used for billing.

PlugNPay per Transaction Fee Structure

PlugNPay transaction cost is based on monthly transaction volume within your organization. The following table provides PlugNPay's *per transaction* cost as of February, 2012.

> **Note:** The data in the table below is subject to change by PlugNPay. Be sure to confirm this information when contracting with them.

Monthly Transactions	Cost/Transaction in US cents
Fewer than 1,000	$0.075
1,000 – 5,000	$0.05
Monthly Minimum per Gateway	$15.00

Your monthly transaction total is the sum of all credit card transactions from every point of sale within your organization; transactions from your individual point of sale workstations are not billed separately.

For Example: You have two (2) facilities each with two (2) points of sale. During May, Facility 1 processes 6,500 transactions through PlugNPay and Facility 2 processes 4,000 transactions through PlugNPay. Beginning in June, your per transaction cost will be 0.05 because your organization processed 10,500 total *transactions in May. It will remain at 5 cents/transaction for at least the next three (3) months. See below for further details.*

Raising or Lowering Your per Transaction Fee

Lowering Your per Transaction Fee

PlugNPay does not monitor your transaction volumes on a regular basis. It is therefore up to you as a customer to notify PlugNPay when you attain a higher transaction threshold and thus qualify for a better per transaction rate.

As a customer, you will always start at the 7.5 cents per transaction ($0.075/transaction) rate. Once you reach the 1,000 transaction/month threshold level YOU must inform PlugNPay, so that your per transaction fee can be reduced to match the proper rate beginning the next month.

PlugNPay will provide the instructional steps required to monitor your transaction volume.

Raising Your per Transaction Fee

To help offset seasonal dips in sales, PlugNPay provides a three (3)-month buffer at your current per transaction rate before changing it, should your transaction volume drop to a lower threshold number (and thus affect a higher per transaction rate).

For Example: You hit the 1,000/month transaction threshold in June and qualify for the $.05 /transaction rate starting in July. Sales remain constant through the summer months, but in September your sales drop below the 1,000-transaction threshold. You will still be charged the 5 cent per transaction fee for September. This will be true for October and November as well if your volume remains below the 1,000-transaction threshold. If the volume stays below 1,000 in December, you will revert to the 7.5 cents per transaction rate.

Setting Up Your System to Use PlugNPay WebXPress

Note: The following steps assume you have a valid PlugNPay user account. If you do not have a PlugNPay account, you cannot proceed. To establish a PlugNPay account, contact Barbara Volpe at PlugNPay: (800) 945-2538 x7738 or barbara@plugnpay.com.

In order to use PlugNPay credit card processing, you will need to complete the following setup steps:

- Set up your PlugNPay WebXPress device.
- Link the appropriate Credit Card device in the Device Hierarchy.
- Set up and link your MSR device, if applicable
- Install the MagTek IPAD pinpad hardware, if applicable
- Setup and link your MagTek IPAD Pinpad device, if applicable.
- Run the credit card initialization program.

Note: If you are using the MagTek IPAD pinpad, you must install the hardware BEFORE proceeding with the RecTrac setup. Refer to Appendix A - MagTek IPAD for setup instructions and then return here.

Set Up Your PlugNPay WebXPress Device

1 Go to File Maintenance • System • Device Maintenance • Printer/Device Maintenance.

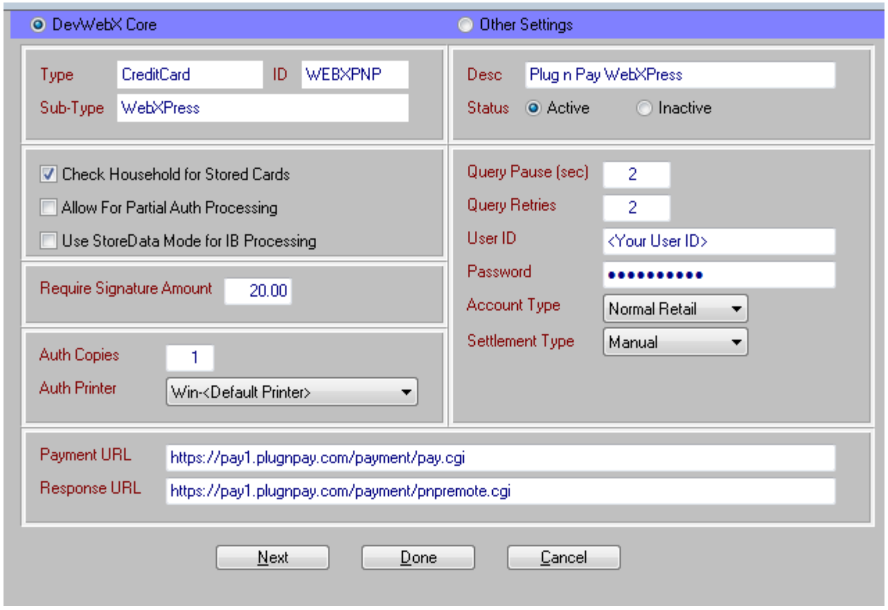
2 Click Add.

3 Select **CreditCard** as the device *Type*, and **WebXPress** as the *Sub-Type*.

4 Type an ID for this device. *For example, WEBX*. Click **Next**.

5 Type a Description for this device. *For example, WebXPress CC processing*.

6 Select **Active** as the *Status*.



7 If the *Check Household for Stored Cards* option is selected and the customer has previously used a credit card, the clerk processing the transaction will receive a list of credit cards (masked) that the customer has previously used. Once the clerk chooses a card from the list, the last order ID, as well as the masked credit card information is passed to PlugNPay to validate the sale. If the stored information is verified the sale will be permitted. If the stored information is not verified the sale will be declined.

8 *Use File Method for Results:* This option is for customers that wish to use the File Drop method for credit card authorizations. The File Drop method can be used as an alternative to direct authorizations, and requires a shorter Internet connection time. For more information regarding this process contact VSI Customer Support.

9 *Use StoreData Mode for IB Processing:* This is a temporary option that, if selected, will bypass the $0.00 charge to validate a credit card, and instead will simply charge the credit card without first validating any stored information for recurring billing purposes. **This option is not typically selected, unless you've instructed to do so by a VSI representative.**

10 Query Pause: Enter a numerical value. The number you enter is the number of seconds RecTrac will wait, after the clerk clicks "Close," before allowing the clerk to process another transaction. This "pause" will ensure the transaction completes on the PlugNPay website.

Note: VSI recommends a Query Pause of 1-2 seconds.

11 Query Retries: Enter the number of times to loop through for a good response from PlugNPay. This number works in conjunction with the Query Pause value. The recommended entry for this field is *2*.)

> **Note:** If there is no response, or the response for a transaction is a failure (declined), then it looks to the Query Retries value. If the Query Retries field is set to '0', and the response is a failure, the transaction is done and there will be no retry

12 Enter your PlugNPay Account **User ID** and **Password**.

If you opt to use Remote Client Password (highly recommended), you will need to generate a new password while on the PlugNPay website and enter it in the *Password* field. Refer to Set Up Remote Client Password for further information.

> **Note:** Failure to enter the correct User ID and/or Password will result in failed (No Authorization) credit card transactions on the PlugNPay site. Users running RecTrac 10.1n (or later) will receive a pop-up message indicating the cause of the transaction failure. Users NOT running 10.1n (or later) will not receive this message. See Troubleshooting below for further information.

13 Select your account type for this device: **Normal Retail, E-Commerce** or **Restaurant**.

14 Enter the desired Settlement Type: **Auto** or **Manual**.

> **Note:** VSI recommends selecting *Auto* unless you want to do Tip Processing via a restaurant account. You must be running RecTrac version 10.1n (or later) to perform Tip Processing. See also Settling Options in RecTrac and PlugNPay below.

15 *Require Signature Amount*: Enter a threshold amount for requiring a signature on Credit Card purchases, such as *$20.00*. Sales that do not meet this amount will bypass the signature screen and "Signature Not Required" will be printed on receipts. Receipts for sales that meet or exceed the threshold amount will be printed with a signature line for the patron.

16 *Authorization Copies*: Enter the number of Authorization (Receipt) Copies you would like to print with each credit card transaction.

17 Select the appropriate *Authorization (Receipt) Printer*.

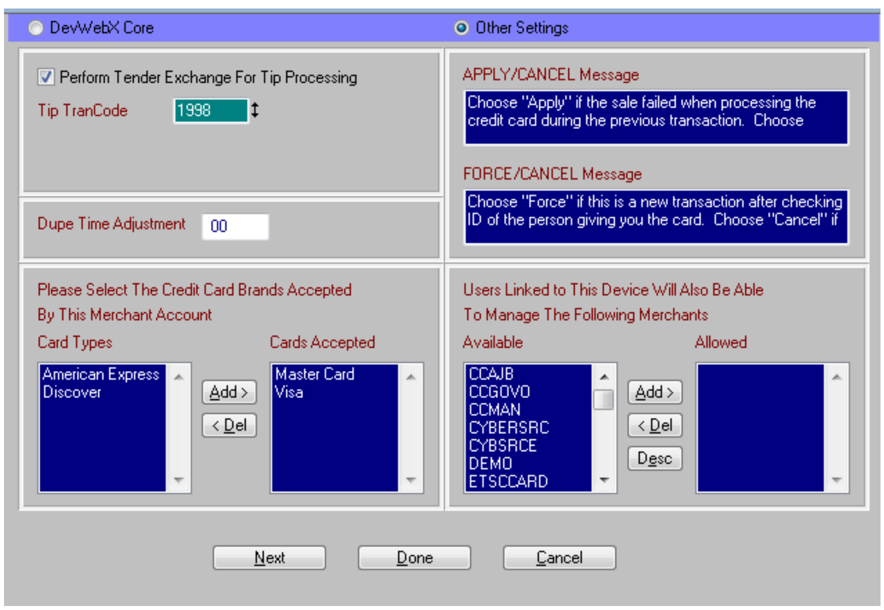
Important Note! If your organization uses a single credit card device for multiple workstations that do NOT all share the same authorization receipt printer, you must additionally link an AUTHRCPT device at the Workstation level of the device hierarchy for each workstation that uses a different authorization receipt printer. Configure each AUTHRCPT device to use the specific printer for each workstation. **Failure to do this will cause receipts to take an abnormally long period of time to print.** Linking an AUTHRCPT device will override the authorization printer linked to the credit card device.

18 Enter the following in the Payment URL field: https://pay1.plugnpay.com/payment/pay.cgi

19 Enter the following in the Response URL field: https://pay1.plugnpay.com/payment/pnpremote.cgi

Note: These fields must be entered exactly as displayed. See also Workstation Requirements above.

20 Click **Next** to proceed to the Other Setting screen.



21 Choose *Perform Tender Exchange For Tip Processing:* If the Account Type is *Restaurant*, then you may enable this toggle if your wait staff/bar staff takes cash from the drawer for their credit card tips.

22 Right-click or press **F9** in the Tip TranCode field to select your Tip Tran Code, if necessary. You will only use the Tip Tran Code field if your Account Type is *Restaurant*.

23 Credit Card transactions are date/time stamped using Greenwich Mean Time (GMT). The *Dupe Time Adjustment* setting is used to adjust credit card transaction times so they display in "real" time based on your time zone. Enter the number of hours your time zone is behind/ahead of GMT in this field. *For example, if your time zone is Eastern Standard Time (EST), you would enter* -5.

> **Note:** Greenwich Mean Time does NOT change with Daylight Savings Time. Therefore, you must adjust this field whenever you are in Daylight Savings Time. *For example, if your time zone is Eastern Daylight Savings Time (EDT), you would enter* -4 *in this field to account for the hour you "spring ahead."*

24 Using the first set of dual selection lists, highlight the credit card brands that will be accepted by your organization, and click the **Add>** button to place them in the *Cards Accepted* column.

25 The default *Apply/Cancel* message is:

"Choose "Apply" if the sale failed when processing the credit card during the previous transaction. Choose "Cancel" if this is a new transaction and the credit card does not belong to the person after checking ID."

For example, a credit card sale fails during the transaction. The clerk then runs the sale again with the same card/same dollar amount. If the dollar amount and the credit card number being passed to PlugNPay match a sale in RecTrac that does NOT have an order ID, the system will ask the clerk if they want to add the order ID from the PlugNPay site to the previous transaction in the rpcctxns table.

26 The default Force/Cancel message is:

"Choose "Force" if this is a new transaction after checking ID of the person giving you the card. Choose "Cancel" if this is a new transaction and the credit card does not belong to the person after checking ID."

For example, if you purchase something with a credit card and the charge is $5.00, and then shortly after making that purchase, you make another purchase for exactly $5.00 using the same credit card number. PlugNPay will identify that as a duplicate charge (and potential fraud), pass it back to RecTrac and display the Force/Apply Message. This message warns the clerk that the card was already charged and allows them to decide if it should really be charged again.

27 Using the second set of dual selection lists, highlight the merchants that any user linked to this device will also have the authority to manage, and click the **Add>** button to place them in the *Allowed* column.

28 Click **Done**. You will return to Device Maintenance.

29 Repeat Steps 2-28 for each additional WebXPress Credit Card device needed for your organization.

> **Note:** PlugNPay will issue unique User IDs and Passwords for each separate credit card terminal you required. For example: You accept credit cards at the Fitness Center and at the Rec Center, and you require each installation to run its own financial reports. You will require two (2) PlugNPay User IDs for this scenario and, thus, two (2) WebXPress credit card devices.

25 Click **Exit** when finished to return to the main RecTrac menu.

Link the PlugNPay WebXPress Device in the Device Hierarchy

1 Go to File Maintenance • System • Device Maintenance • Device Assignments.

2 Decide on which level (User, Menu, Workstation, Default) of the Device Hierarchy to link the device. If you are unsure of the best level to link a device, please call Vermont Systems Customer Support (1-877-883-8757) for help.

3 Expand the appropriate level and then highlight the appropriate user, menu or workstation

4 In the **Device Type** select **Credit Card**.

5 In the **Device to Add** field select the appropriate PlugNPay WebXPress device. Click **Add to Linked Devs**.

6 Repeat Steps 2-5 for all users, or menus or workstations or defaults that will use this device. Click **Exit** when you are finished.

> **Note**: Anytime you change a credit card device assignment, you have to stop and restart your WebSpeed (wsrtlive and wsrtdemo) and AppServer (asrtlive and asrtlivesch) brokers in OpenEdge (Progress) Explorer tool. Contact VSI Customer Support if you require assistance with this procedure.

Set Up Your MSR Device

Perform these steps only if you use Magnetic Stripe Readers. Otherwise, proceed to Enable the Smart ERI Paycode Feature on your Payment Device(s) below.

> **Note:** If you are using the MagTek IPAD device, you will not link a MSR device. Proceed to Enable the Smart ERI Paycode Feature on your Payment Device(s) below.

1 Go to File Maintenance • System • Device Maintenance • Printer/Device Maintenance.

2 Highlight the **MSR** device and click the **Change** button.

3 You will continue to the Wedge Core Information screen.

4 Select the **Pause After Swiping** toggle if you want to review the credit card information after you swipe the card and before you click the Authorize button. De-select this option if you want to skip the review and have the system automatically authorize the sale.

5 Select the **Use Automatic Parsing** option to automatically determine the credit card number and expiration date layout. Deselect this option to manually change the CC# Layout and Exp Date Layout fields.

CC # Layout – This field is used to specify where and how to identify the credit card's account number. You must specify the delimiting character within the scanned data, and which field number (in relationship to all other scanned fields) contains the card's account number, as well as maximum length that this field can be. The field format is dependent on the credit card reader type.

Exp Date Layout – This field is used to specify where and how to identify the credit card's expiration date. You must specify the delimiting character within the scanned data, and which field number (in relationship to all other scanned fields) contains the card's expiration date, as well as maximum length that this field can be. The field format is dependent on the credit card reader type. RecTrac will always take the digits 3 and 4 to be the month of the exp date and digits 1 and 2 to be the year of the exp date. The swiper must be setup to read YYMM for this to work correctly.

6 Click **Done**.

Link the MSR Device in the Device Hierarchy

1 Go to File Maintenance • System • Device Maintenance • Device Assignments.

2 Decide on which level (User, Menu, Workstation, Default) of the Device Hierarchy to link the device. VSI recommends that you link the MSR device at the workstation level of the hierarchy. If you are unsure of the best level to link a device, please call Vermont Systems Customer Support (1-877-883-8757) for help.

3 Expand the appropriate level and then highlight the appropriate user, menu or workstation

4 In the **Device Type** select **MSR**.

5 In the **Device to Add** field select the appropriate MSR device. Click **Add to Linked Devs**.

6 Repeat Steps 2-5 for all users, or menus or workstations or defaults that will use this MSR device. Click **Exit** when you are finished.

Enable the Smart ERI Paycode Feature on your Payment Device(s)

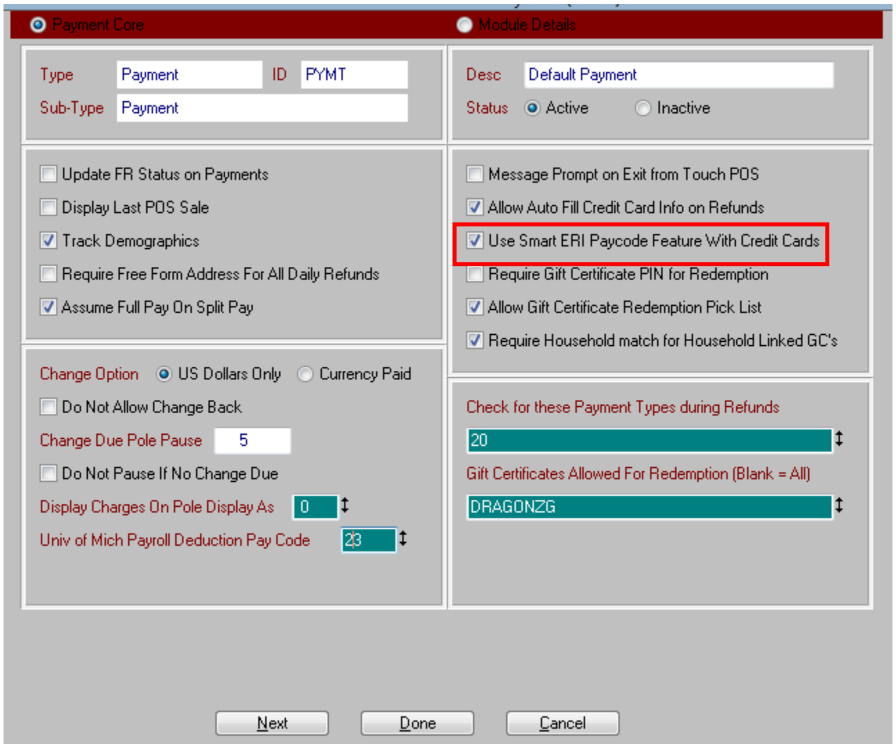
Enable the **Use Smart ERI Paycode Feature With Credit Cards** on *all* Payment devices used to process Credit Card/Debit Card transactions.

This feature will match a credit card's prefix automatically to its corresponding pay code in RecTrac when processing a sale with PlugNPay regardless of the initial credit card pay code used. This is useful when using ERI because RecTrac is no longer storing or capturing credit card numbers during sales/authorizations and is unable to validate the prefix at the time the credit card is swiped or keyed in.

1 Go to File Maintenance • System • Device Maintenance • Printer/Device Maintenance

2 Highlight/Select a Payment device and click **Change**.

3 Enable the **Use Smart ERI Paycode Feature with Credit Cards** toggle, which is located on the right-hand side of the Payment Core screen.



4 Click **Done** to return to Device Maintenance.

5 Repeat these steps for every Payment device that will be used to process Credit Card/Debit Card transactions.

6 Click **Exit** when done.

Alternate Credit Card Pay Codes for Reporting by Card Type

You do not need to alter your current Pay Code set up to process credit cards using the Smart ERI Paycode Feature. The "standard" RecTrac set up where Pay Code 3=Visa/Master, Pay Code 4= Amex, Pay Code 5=Discover, for example will work PROVIDED you do not need to report sales by specific credit card type. Using the Smart ERI Paycode feature will automatically link VISA/MasterCard sales to Pay Code 3 and AMEX sales to Pay Code 4 (assuming your setup follows the example) and you can run sales reports as you did previously.

However, if you are required to report by credit card type, VSI recommends creating new pay codes for your credit card sales. Smart ERI Paycode will allow you to process credit card sales using your traditional pay codes (3, 4, etc…), so there will be *no operational difference* for your organization. Behind the scenes, RecTrac will link the card to the appropriate pay type.

If you choose to create alternate pay codes, you will:

- Go to Pay Code Maintenance, select and change existing Credit Card pay codes, <u>DELETE</u> all information in the Prefix Validation field (remove "3" and "4" from Pay Code 3, for example) and then click Done.

- Create new Pay Codes (type=Credit Card) for the individual credit card types (for example: Pay Code 24=VISA, Pay Code 25=MasterCard, Pay Code 26=AMEX, etc…) and input the lone card prefix in the Prefix Validation field for each card. (For example, Pay Code 24 = VISA, prefix validation =4, Pay Code 25+MasterCard, prefix validation =5, etc…). Exit Payment Code Maintenance when done.
- Add the new Pay Codes to your existing Payment Devices.

If you are unsure of how to create/modify Pay Codes or how to add Pay Codes to your Payment device(s), please call Vermont Systems Customer Support (1-877-883-8757).

Run the ERI CC Conversion Mask Utility

The ERI CC Conversion Mask Utility goes through your RecTrac database and replaces any full (16-digit) credit card number on your Cash/GL/Transaction History records with a credit card mask. Run this program after completing IDI to PlugNPay WebXPress ERI conversion.

Plan Accordingly! Like other aspects of the IDI to ERI conversion, running this utility could take a few minutes to a number of hours depending on the number of records in your database and the speed of the workstation/server on which you are running it.

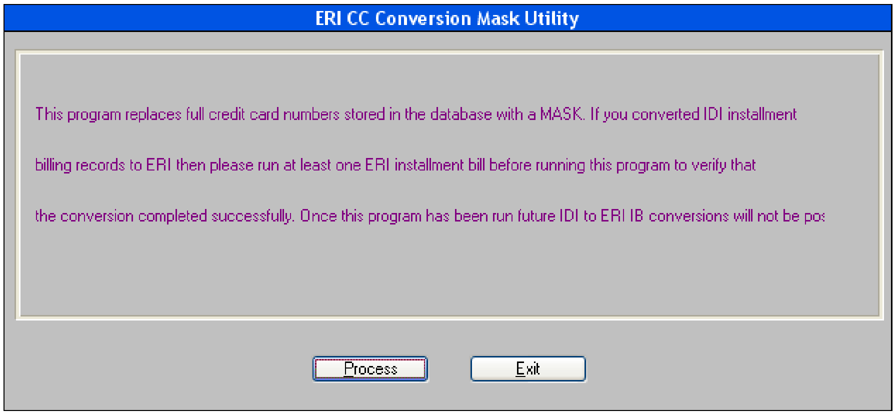
> **Note:** You MUST be running RecTrac 10.2k or greater to complete the process outlined in this document. If you are NOT running RecTrac 10.2k or greater, refer to *IDI to ERI CCard Conversion*. Contact Vermont Systems Customer Support for assistance if you do not know the version of RecTrac you are running.

1 Go to Utilities • System • Custom Program Loader. (If you are in Custom Program Loader, go to step 2.)

2 Enter *ic0617.r* in the **Program To Run** field. There are no **Program Options**. Do NOT select **Run Program Persistent**.

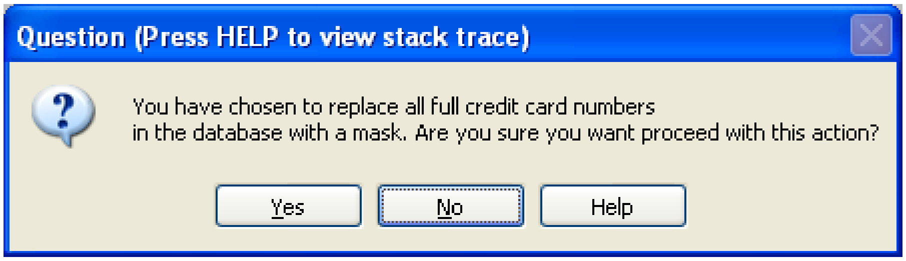
3 Click **OK**. You will proceed to the CC View/Print/Del Permission (User Verification Required) screen.

4 Enter your UserID and Password in the appropriate fields and click **OK**. You will continue to the ERI Mask CC Info Program screen.



5 Read the message text carefully, as it describes what the utility will do and click **Process**.

6 Read the challenge message carefully and answer **Yes** when you're ready to proceed.



7 You will be prompted when the process finishes. Click **OK** and **Exit**. **Exit** Custom Program Loader.

Duplicate Transaction Checking Set Up

Duplicate transactions can occur several different ways. For example, if a clerk closes the payment window before PlugNPay has had a chance to return an authorization code to RecTrac, and the clerk then tries to resend the same transaction amount on the same credit card that was previously used. This could be flagged as a potential duplicate transaction on the PlugNPay side.

To utilize Duplicate Transaction Checking you must enable the "Duplicate Check" option and frequency directly on the PlugNPay site, and then ensure that the appropriate messages are entered on your PlugNPay – WebXPress device(s).

Customers who do Installment Billing with Credit Card Auto-Debit and/or WebTrac E-commerce accounts ***cannot*** use Duplicate Checking. ***DO NOT*** enable Duplicate Check on your PlugNPay Installment Billing Account or on your WebTrac E-Commerce Account.

To Enable Duplicate Check

1 Go to: **https://pay1.plugnpay.com/admin/**

2 Using the Login and Password given to you by PlugNPay, log into your account.

3 Under *Settings*, click **FraudTrak2**.

> **Note:** Contact PlugNPay if you do NOT have the **FraudTrak2** option. They will enable it for you. Enabling FraudTrak2 is free service for Vermont Systems customers. PlugNPay Tel: (800) 945-2538

4 Scroll down to Duplicate Check and place a checkmark in the **Check to enable duplicate checking** box.

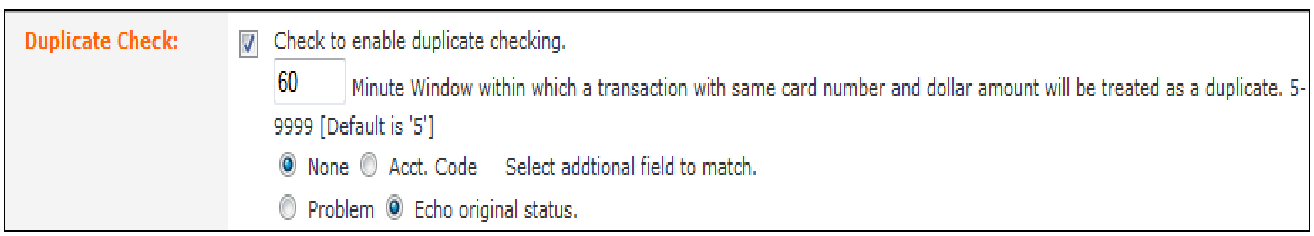
5 Enter the number of minutes between transactions you would like to use when flagging duplicate transactions. *For example, 5*.

6 Ensure the *Echo original status* radio set option is enabled. Do not select *Problem*.

7 Scroll down to the lower portion of the screen and click the **Update Fraud Screen Configuration** button.

8 Log out of PlugNPay.

9 Refer to the Set Up Your PlugNPay WebXPress Device portion of this document for specific details on *Apply/Cancel* and *Force/Cancel* messages found on the second screen of the WebXPress device. These messages will be displayed for clerks depending on the terms of the transaction.



> **Note**: Any potential duplicate transactions will be flagged as “Fraud” on the PlugNPay website. This does NOT mean that a fraudulent charge has been made; rather it is an indication that a charge has been recognized as a potential duplicate.

Installment Billing/Auto Debit Setup

To process installment bills/auto-debit credit cards you will need to setup additional accounts specifically for this purpose. PlugNPay will then flag each of these accounts as 'MOTO' (Mail Order/Telephone Order). Once the account(s) have been setup with your processor, you will need to setup a new **Credit Card device** AND a **Credit Card Re-Direct device** in RecTrac (with a sub-type of RDInstBill) to which you will link the 'MOTO' credit card account. (You will need to do this for each MOTO account that you create.)

The following steps assume that your RecTrac users are setup to process regular credit card transactions, as well as installment bill/auto-debit processes; however, please note if you have a user ID specifically for installment billing/auto-debit purposes ONLY (and the user ID is not used for any other purpose), you do NOT need to link the 'MOTO' Credit Card device to a CC Redirect Device. You can simply link the 'MOTO' credit card device to your installment bill/auto-debit user ID – at the User ID level of the device hierarchy – as a regular credit card device.

Create a Credit Card Device for Installment Billing/Auto-Debit Purposes

To create a Credit Card device for Installment Billing/Auto debit, follow the steps outlined in Set Up Your PlugNPay WebXPress Device with the following exceptions:

1. When creating the device, use the '**MOTO'** account information given to you by your credit card processor.
2. Choose **CreditCard** as the Type, and then choose **WebXPress** as the Sub-Type.
3. In the ID field type a unique code for this device, such as **PNPMOTO**.
4. In the Description field type a description such as, **PNP ERI Auto-Debit Device**.
5. Expand the *Account Type* drop-down list and select **Normal Retail**.
6. If your organization uses a single credit card device for multiple workstations that do NOT all share the same authorization receipt printer, you must additionally link an AUTHRCPT device at the Workstation level of the device hierarchy for each workstation that uses a different authorization receipt printer. Configure each AUTHRCPT device to use the specific printer for each workstation. **Failure to do this will cause receipts to take an abnormally long period of time to print.** Linking an AUTHRCPT device will override the authorization printer linked to the credit card device.

Create a Credit Card Redirect Device

1. From within Device Maintenance, click **Add** to create a Credit Card Re-Direct device to which you will link the credit card device you just created.
2. From the Type drop-down list choose **CC-Redirect**.
3. From the Sub-Type drop-down list choose **RDInstBill**, and click **OK**.
4. Type a unique ID for this device, such as **PNPIBRDCT**.

5 Click **Next.**

6 Type a description for this device, such as **PNP Auto-Debit CC Re-Direct**.

7 From the *Primary IB Device* drop-down list, choose the Credit Card Device you just created. Using our example you would choose **PNPMOTO**. (Leave the *Use Secondary PNP Device* field set to <None>.)

8 Click **Done,** and then click **Exit** to return to the main menu.

Link the Credit Card Redirect Device

A Credit Card redirect device MUST be linked within the device hierarchy for the login ID that will be performing installment bill/auto-debit functions. For this reason it is recommended that this device is linked at the *Defaults* level of the hierarchy.

1 From the main menu, go to: File Maintenance • System • Device Maintenance • Device Assignments.

2 Click the '+' next to Defaults and highlight Default Devices. (Depending on your device structure you may link the CC-Redirect device at the User ID, Menu Group or Workstation level instead.)

3 Click the **Device Type** drop-down arrow and choose **CC-REDIRECT**.

4 Click the **Device to Add** drop-down arrow and choose the CC-REDIRECT device that you previously created. In our example we would choose **PNPREDIR**.

5 Click **Add to Linked Devs**. Click **Exit**.

Using PlugNPay WebXPress

Account Setup for Using the PlugNPay Website

Prior to using the PlugNPay website, perform the following instructions for the appropriate configuration.

1. Go to: **https://pay1.plugnpay.com/admin/**
2. Using the Login and Password given to you by PlugNPay, log into your account.
3. Under *Settings*, click **Security Administration**.
4. On the Security Administration Area screen, click **Transaction Security Configuration**.
5. Scroll down to the Add IP Addresses section near the bottom of the screen, and type your organization's public IP address(es). (If you do not know your public IP address, you can obtain it by going to: **http://whatsmyip.org**)
6. Click **Add IP Address**.
7. Repeat steps 5 & 6 for EVERY public IP address your organization uses and/or through which you will process PlugNPay Transactions.:
8. Close the window when done by clicking the 'x' in the upper right-hand corner of the screen. **See also: Require IP Match below.**

> **Note:** Failure to register your public IP address(es) with PlugNPay will result in failed (No Authorization) credit card transactions on the PlugNPay site. Users running RecTrac 10.1n (or later) will receive a pop-up message indicating the cause of the transaction failure If applicable, that pop up will include the IP Address that is NOT registered. Users NOT running 10.1n (or later) will not receive this message. See Troubleshooting below for further information

9. Under *Settings*, click **Account Settings**.
10. Click on **Payment Script Config** and then put a check mark next to **Skip Summary Page**.
11. If your organization will be processing Installment Bills/Auto-Debit Transactions/Tee Time No Shows, etc…, put a check mark next to **Allow Checkcard Orders**. (Under the *Payment Script Config Options* section.) If your organization does not process Installment Bills/Auto-Debit Transactions/Tee Time No Shows, etc…, you may skip this step.

> **Note:** The word "Checkcard" does NOT refer to a credit card type, such as the VISA Checkcard, but rather means that a customer's regular credit card will be checked

for validity. With this feature enabled, PlugNPay will do a $1.00 transaction against the card swiped into the Household (HH Update • Financial Info • Credit Card Info • Add) to ensure the card is valid. The $1.00 transaction will then be voided immediately.

12 Click the **Update Settings** tab located under *Transaction Admin Options* and then close the window by clicking the **X** in the upper right-hand corner of the screen.

13 Before going live with PlugNPay, you must determine how you wish them to bill you for their services. You can elect to pay your monthly fees by credit card or electronic ACH debit.

- **Click on link labeled** Billing Authorization**, which is located in the *Settings* section.**

Set Up Remote Client Password

Using a Remote Client Password for your VSI software will prevent any interruption to transaction processing if your main PNP administration password is ever changed. Remote Client Password requires you to generate a new password while on the PlugNPay website and then enter that password in the appropriate field on your WebXPress Credit Card device(s).

VSI *HIGHLY* *RECOMMENDS* using this option.

To setup a Remote Client Password:

1. From the PlugNPay website, log into the Admin area of your PlugNPay account.
2. Click the **Security Administration** link.
3. Click the **Username/Password Configuration** link.
4. Scroll to *Remote Client Password* section.
5. Select the **Generate Random Password** checkbox.
6. Click the **Add/Edit Remote Password** button. A password will be displayed in the *Remote Client Password* field.
7. Copy the password down on a separate piece of paper immediately. This is ONLY time that password will be available.
8. Enter the password from step 6 into the *Password* field on your WebXPress Credit Card device(s) (steps provided below) and then continue with the PlugNPay setup, Install Deftran.html as Your Transition Page.

To enter the Remote Client Password into your WebXPress Credit Card device(s)

1. Login to your VSI software (RecTrac or CYMS)
2. Go to File Maintenance • System • Device Maintenance • Printer Device Maintenance.
3. Click on the *Type* column header and then press the letter 'C' on your keyboard.
4. Scroll down the browser to your Credit Card devices and highlight/select your first WebXPress Credit Card device and click **Change**. "WebXPress" will be listed in the *Sub-Type* column.
5. The *Password* field is located on the right-hand panel of the device. Highlight and delete the existing password. Then enter the password that was generated in step 6 of the Remote Client Password steps above.
6. Click **Done**.
7. Repeat steps 4-6 for each remaining WebXPress Credit Card device in your database.

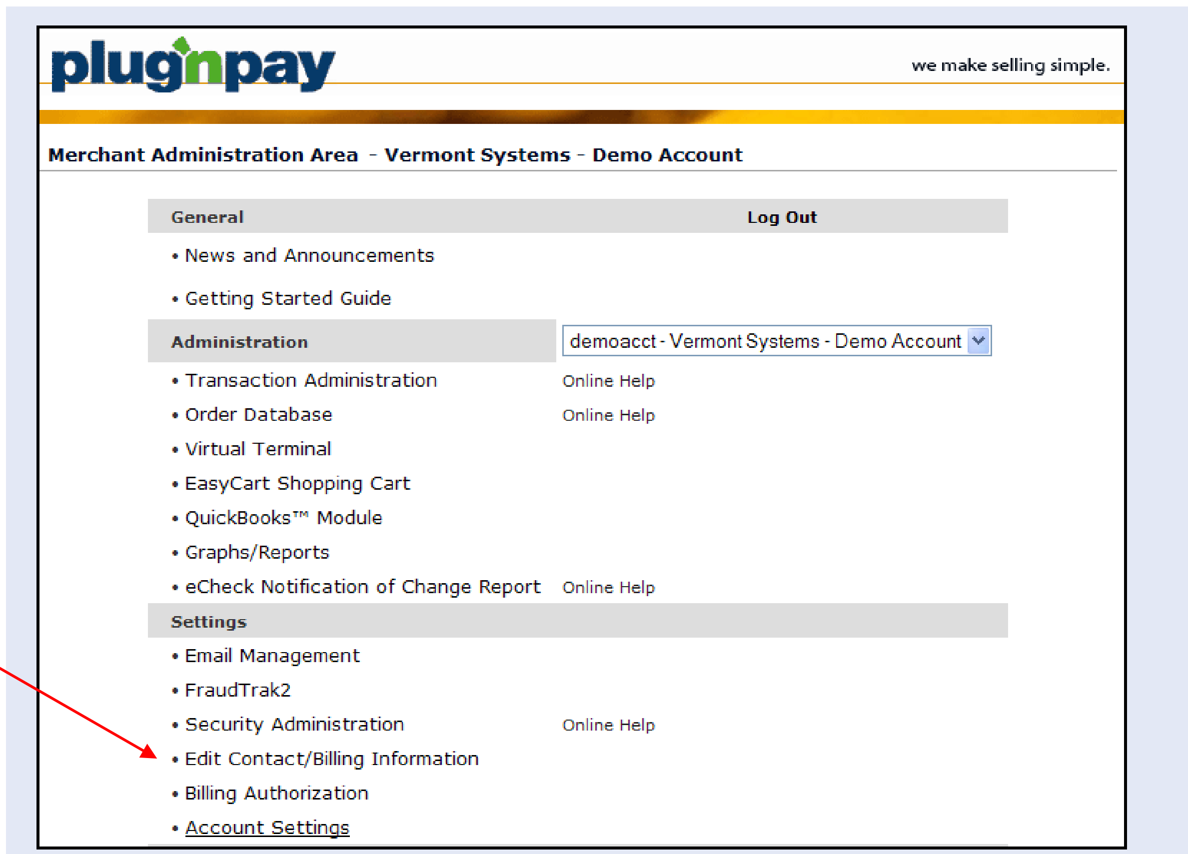
8 Exit RecTrac (or CYMS) and log back in on each workstation to which these credit card devices are linked for your changes to take effect.

Install Deftran.html as Your Transition Page

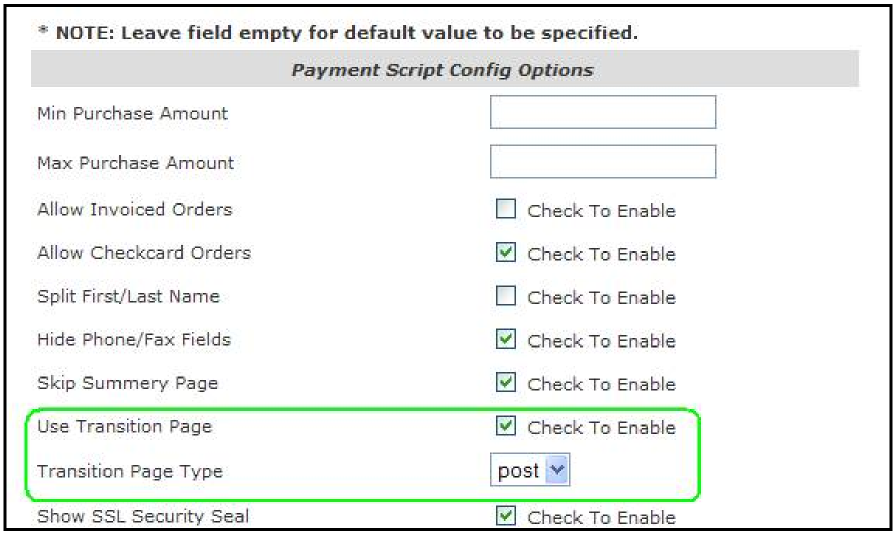
Follow the steps below and ensure your transition pages look like the examples presented.

1 Go to the Account Settings page and enable the *Use Transition Page* toggle and Set Transition Page Type = *POST* as shown below:

- **Login to your PlugNPay Account online and go to Settings • Account Settings • Click** Payment Script Config

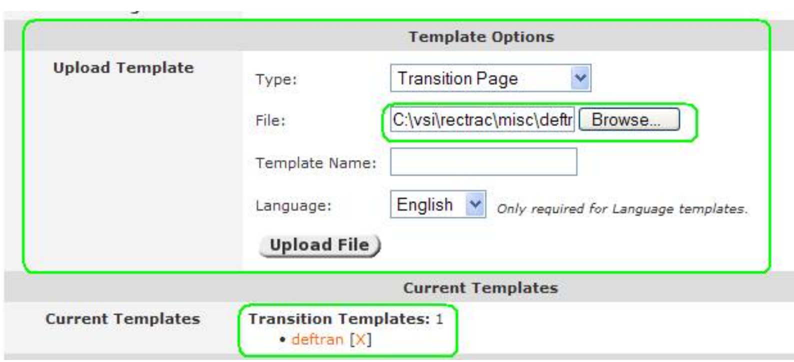


- **Place a check mark next to "Use Transition Page"**
- **Use the drop-down list to set Transition Page Type to *POST.***

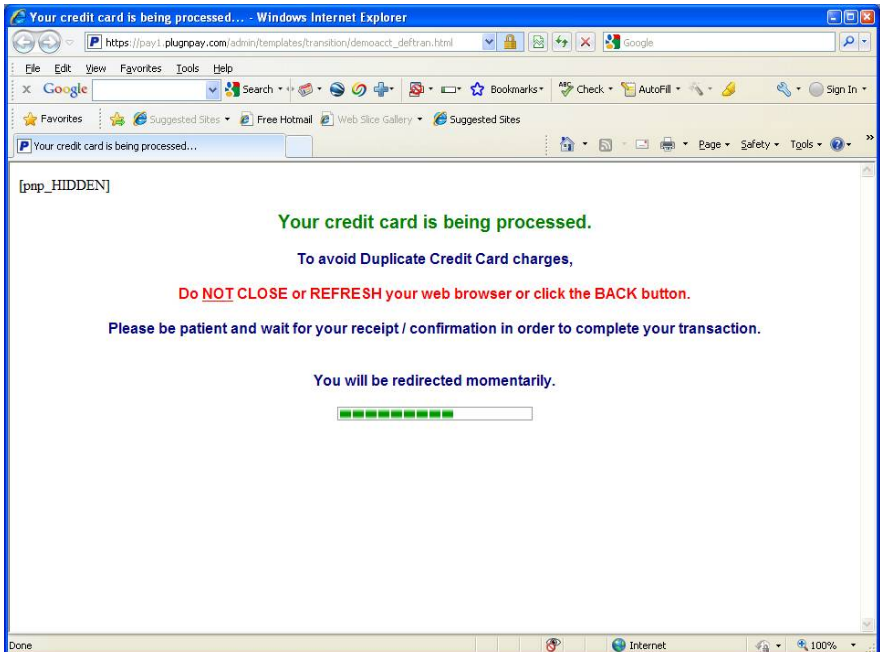


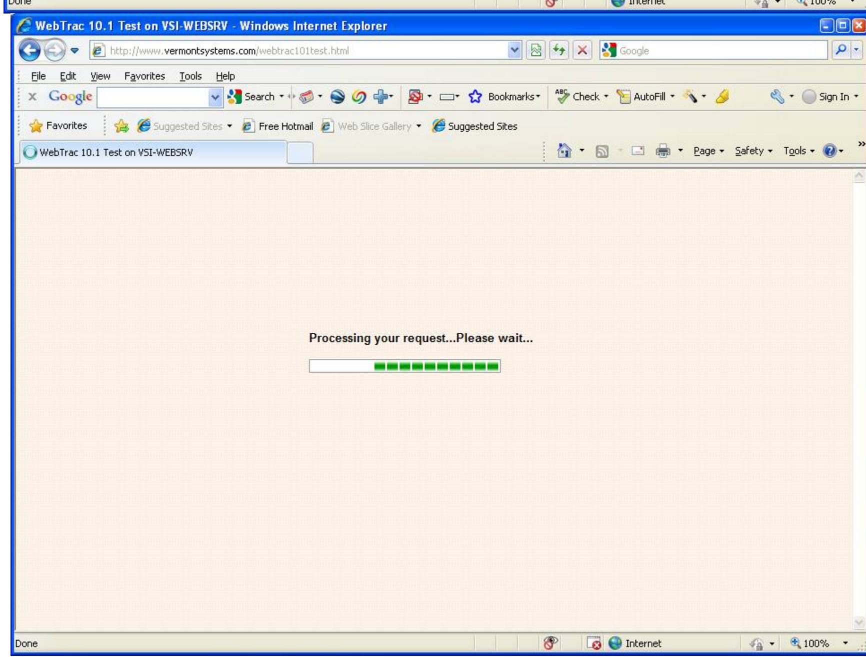
2 Upload the default VSI Transition page to your Account Settings.

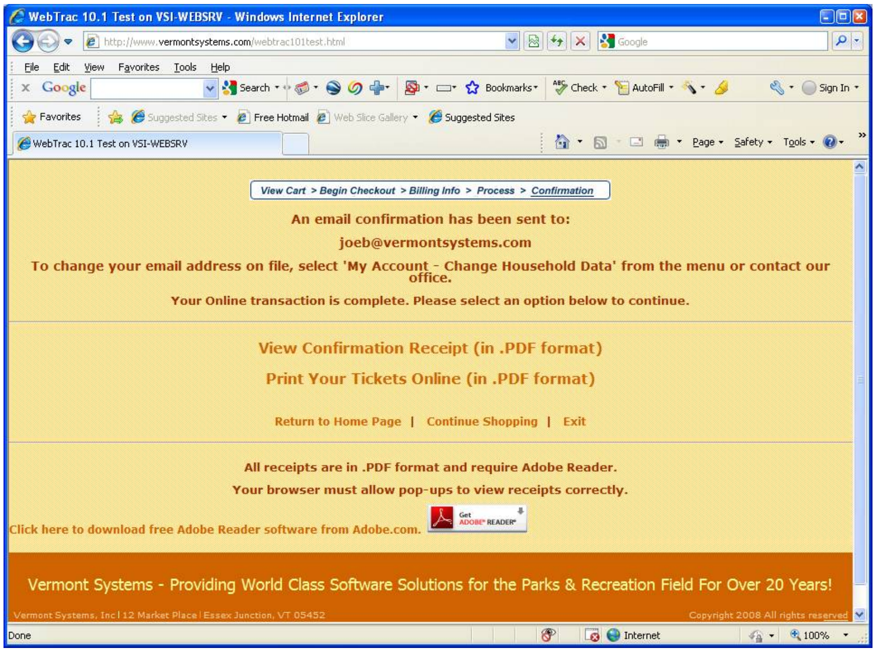
- Login (or go back) to your PlugNPay account and go to Settings • Account Settings
- Near the bottom of the screen you'll find *Template Options.*
- Use the Type drop-down list to select Transition Page.
- Click the browse button. Browse to *deftran.html*. This file is located in the <x:\>\vsi\rectrac\misc directory, where <x:\>= the drive partition on which RecTrac is installed. (This file will be installed when you run the 10.2 update.exe program.)
- Leave template name blank and language as English.
- Click Upload File. You will be prompted when the process is complete.
- After the prompt, save changes and exit.
- Go back into your PnP Account Settings • Template Options section.
- Look at the Current Templates section and verify that your Transition Templates = *deftran*.



When processing a transaction in WebTrac with the *deftran* transition page in place, you will see the following screen transition before being redirected back to the WebTrac payment processing programs:







PlugNPay Fraud Track

Before exiting the PlugNPay website, be sure to ENABLE the ‘Skip IP frequency check’ toggle on the Fraud Track screen.

Customers who do Installment Billing with Credit Card Auto-Debit and/or WebTrac E-commerce accounts ***cannot*** use Duplicate Checking. ***DO NOT*** enable Duplicate Check on your PlugNPay Installment Billing Account or on your WebTrac E-Commerce Account.

1. From the PlugNPay admin screen, click the **Fraud Track** link, which is located in the *Settings* section. You will continue to the Fraud Track page.
2. Find **IP Address Frequency Check:** on the left-hand side of the screen.
3. Enable the toggle next to the **Check to skip IP Frequency check, OR…** line.
4. Click the **Update Fraud Screen Configuration** tab.
5. Exit the browser (click the **X** in the upper right-hand corner of the screen and logout/exit the PlugNPay website.

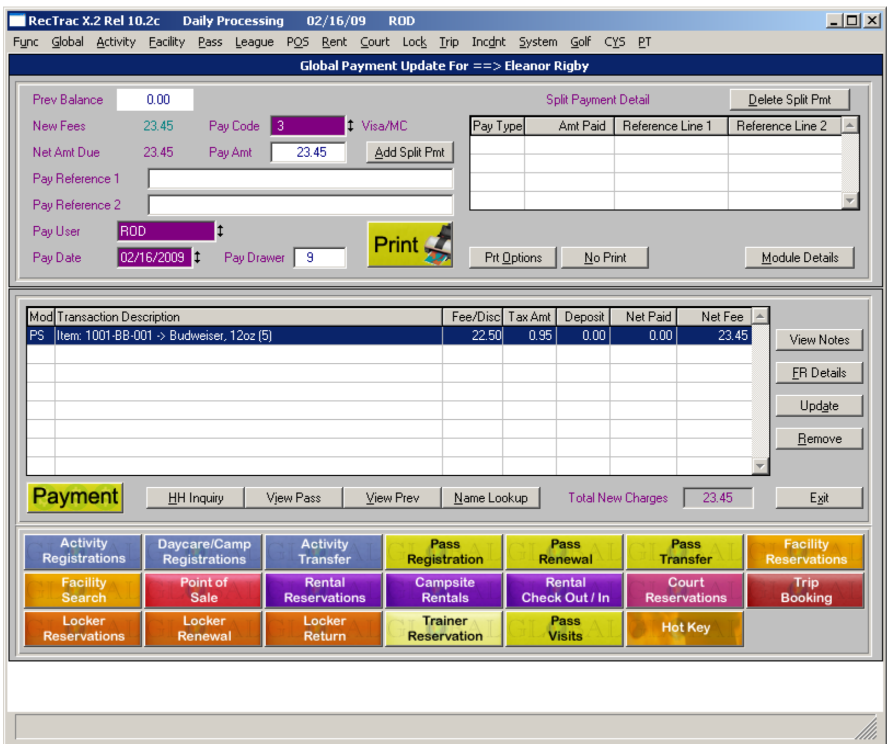
> **Note:** Failure to disable FraudTrack may result in transactions not being processed due to high volume. VSI recommends disabling this feature. See Troubleshooting below for further information

Processing Transactions in RecTrac Using PlugNPay ERI

> **Note**: Duplicate transaction logic has been added to PlugNPay credit card processing. If a duplicate transaction is found the program will prompt you to do one of the following: 1) apply the previous duplicate to the current sale (as long as there isn't already an rpcctxns record with that order ID), 2) force the transaction through as a separate sale, or 3) cancel back to the payment screen.

Processing a Sale in RecTrac

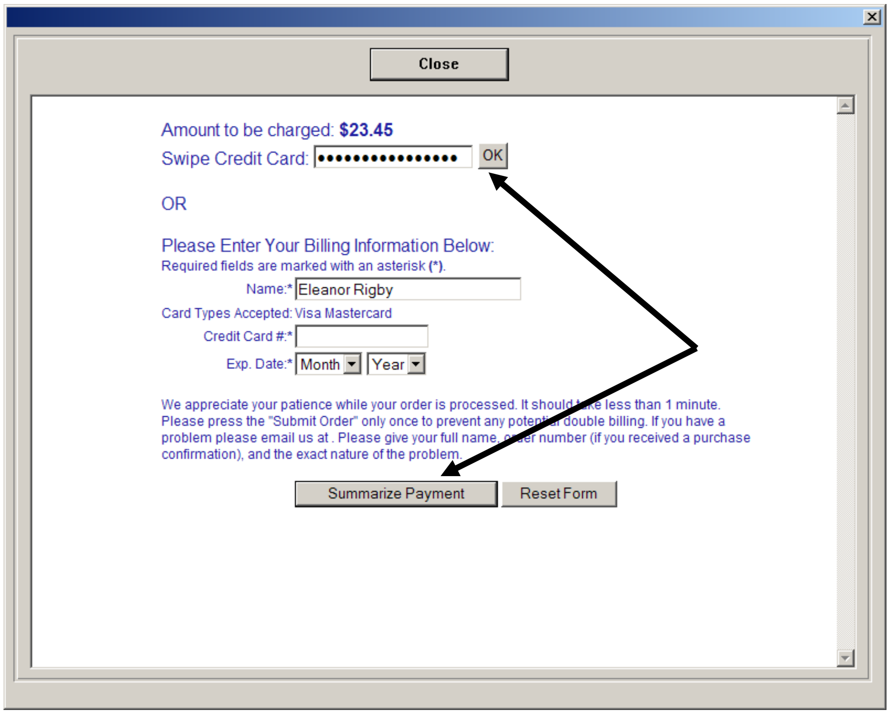
1 Process the sale normally and enter your Credit Card pay code (for example: 3).



2 Click **Print** (or **No Print**).

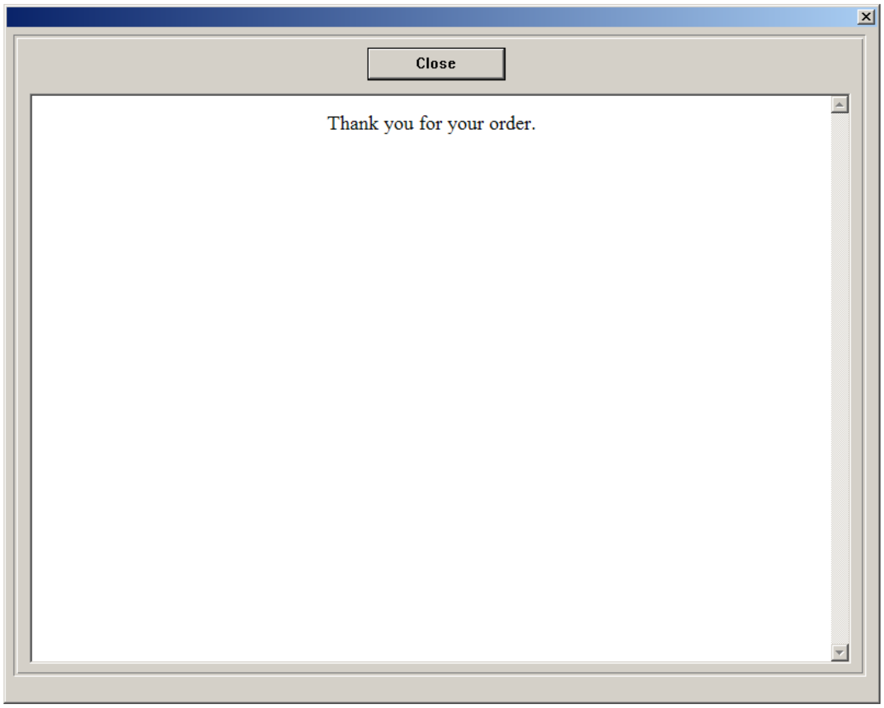
At this point, your web browser launches automatically, and the ERI redirects the operator to a secure web portal so that the card data can be entered and processed.

> **Note:** No card data is entered on a VSI screen and no card data is stored in a VSI application other than the card mask (first 6 & last 4 of the card number).



3 The card data is entered (swiped or manual) on the secure web portal screen. The clerk (or WebTrac customer) clicks **Summarize Payment**.

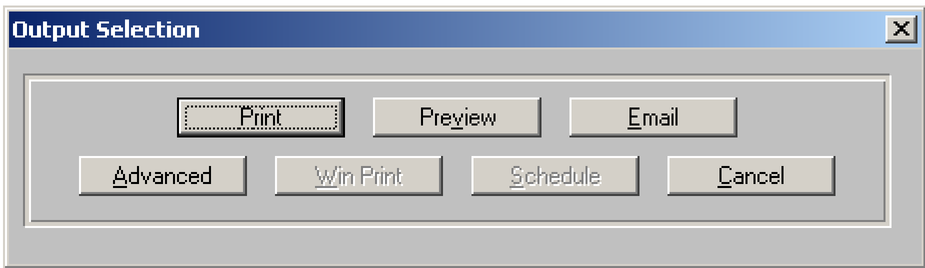
4 The secure web portal sends all card data plus the transaction amount to your processor and awaits a response.



5 The processor authorizes the transaction and sends back a status to the secure web portal that is then interpreted accordingly by the VSI application. The clerk clicks **Close** to exit the PlugNPay portal.

> **Note:** If you do NOT visit this screen but rather are returned immediately to the **Output Selection** screen in RecTrac after clicking Submit Payment, the transaction was NOT successful.

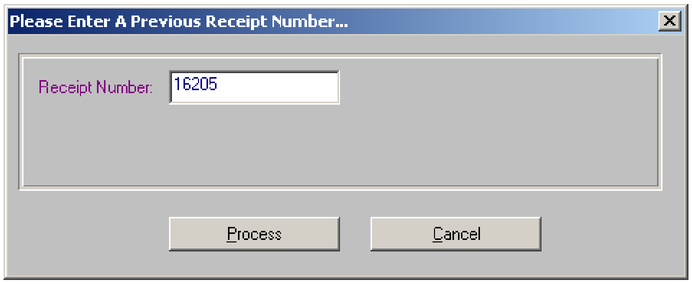
6 The VSI application completes the transaction prompts the clerk for a receipt. You will know the transaction was successful when you see the **Output Selection** screen. Choose your receipt option from the **Output Selection** screen to complete the sale.



> **Note:** If you choose not to Preview Receipts, you will go directly to the **Change Due** screen.

Processing a Refund in RecTrac

1 The RecTrac operator selects credit card as the refund method and clicks **Print**. A receipt number field appears.



2 Enter a receipt number from a previous sale made to the credit card for which you are processing the refund. Ideally this will be the original receipt for which the return is being processed, but *any* receipt for that same credit card is acceptable.

3 Once the receipt number is entered, click **Process**. You will proceed to a challenge message asking whether the credit card mask displayed (the first four (4) and last two (2) digits of the credit card found by the receipt number) is the correct card.

If **Yes**, the refund will be processed and the transaction completed. The Change Due screen will appear. You will not be taken to the PlugNPay portal.

If **No**, you will return to Step 2 above where you can enter a new receipt number.

Processing a Tip in RecTrac

> **Note:** In order to process tips via PlugNPay ERI, you must be running RecTrac 10.1n (or later). Your WebXPress credit card device should be set to Account Type=Restaurant, Settlement Type=Manual and the Tip TranCode field on the device should be populated.

1 Go to Daily Processing • Credit Card Processing • Tip Processing and process the tip as normal.

2 Settle the batch via your Credit Card terminal. Go to Daily Processing • System • Credit Card Processing • Credit Card Terminal. See SettlementOption2: Credit Card Terminal below for details.

Processing Blind Transactions via the PlugNPay Website

Processing a Blind Sale via the PlugNPay Website

1. Go to: **https://pay1.plugnpay.com/admin/**
2. Using the Login and Password given to you by PlugNPay, log into your account.
3. Under *Administration*, click **Transaction Administration**.
4. Scroll down to the *Manual Authorizations & Returns* section.
5. Complete the appropriate information and be sure that the *Type* is **Authorize**.
6. Click **Submit Payment**.

Processing a Blind Refund via the PlugNPay Website

1. Go to: **https://pay1.plugnpay.com/admin/**
2. Using the Login and Password given to you by PlugNPay, log into your account.
3. Under *Administration*, click **Transaction Administration**.
4. Scroll down to the *Manual Authorizations & Returns* section.
5. Complete the appropriate information and be sure that the *Type* is **Return**.
6. Click **Submit Payment**.

Processing a Refund on a Transaction Processed Prior to Using PlugNPay

This process takes care of the refund on the RecTrac side so it displays as though you processed a refund onto the credit card; however, you will need to do a manual credit back onto the customer's credit card by going to the administrative website.

1. Go to: File Maintenance • System • Device Maintenance • Device Assignments
2. At the top left click on the "+" to expand User ID and click on the "+" to expand By ID.
3. Find and highlight your User ID.
4. At the bottom of the screen select Credit Card for Device Type. Then choose "NOVALID" for the device to add.
5. Click on "Add to link Devs" and you should now see it in the box on the right.
6. Exit out of Device Assignments and process a refund onto the credit card.
7. Go back into File Maintenance • System • Device Maintenance • Device Assignments
8. At the top left click on the "+" to expand User ID and click on the "+" to expand By ID.
9. Find and highlight your User ID.

10 Highlight Credit Card = NOVALID and click on **Remove Selected**.

Important Note! Failure to do this step will result in your organization not charging customer credit cards on future transactions.

11 Process a manual credit back onto the customer's credit card.

Refer to: Processing a Blind Refund via the PlugNPay Website

Voiding a Transaction via the PlugNPay Website

1. Go to: **https://pay1.plugnpay.com/admin/**
2. Using the Login and Password given to you by PlugNPay, log into your account.
3. Under *Administration*, click **Transaction Administration**.
4. Under the *Card Queries Void Return* section (near the top of the screen), select the appropriate information for which you would like to perform a query in order to locate the transaction you would like to void. Click **Submit Query**.
5. Click the **Order ID** for the transaction that you would like to void.
6. Click **Void Transaction**. You should receive a message that the transaction has been successfully voided.
7. Close the window by clicking the 'x' in the upper right-hand corner of the screen.

Making a Return Transaction via the PlugNPay Website

1. Go to: **https://pay1.plugnpay.com/admin/**
2. Using the Login and Password given to you by PlugNPay, log into your account.
3. Under *Administration*, click **Transaction Administration**.
4. Under the *Card Queries Void Return* section (near the top of the screen), select the appropriate information for which you would like to perform a query in order to locate the transaction you would like to void. Click **Submit Query**.
5. Click the **Order ID** for the transaction that you would like to return.
6. Click **Return**. You should receive a message that the transaction was successful.
7. Close the window by clicking the 'x' in the upper right-hand corner of the screen.

Submitting a Query for Transactions via the PlugNPay Website

1. Go to: **https://pay1.plugnpay.com/admin/**
2. Using the Login and Password given to you by PlugNPay, log into your account.
3. Under *Administration*, click **Transaction Administration**.
4. Under the *Card Queries Void Return* section (near the top of the screen), select the appropriate information for which you would like to perform a query.

5 Click **Submit Query**.

6 When you are finished reviewing the information, close the window by clicking the 'x' in the upper right-hand corner of the screen.

Settling Options in RecTrac and PlugNPay

Settings in both RecTrac and on the PlugNPay site determine how your credit cards will be settled.

In RecTrac, your settlement options are Auto and Manual. Choose your option on your WebXPress Credit Card device. For normal retail accounts, VSI recommends 'Auto.' For restaurant accounts with Tip Processing, VSI recommends 'Manual.'

PlugNPay controls the settlement setting on their site. You cannot access this setting. By default, the PlugNPay setting is 'No,' meaning they will not initiate a settlement. However, VSI *strongly advises* you contact PlugNPay and confirm their setting for your account.

The following table displays the option settings and settlement result. The VSI-recommended settings appear in ***italics***.

> **Note:** When the PlugNPay settlement option is set to 'Yes/Automatic,' the PlugNPay Settlement is automatic as well. Under certain conditions, automatic settlement on the PlugNPay side can produce incorrect settlement amounts and/or multiple charges to a patron's credit card, most specifically when working with Tip Processing and WebTrac purchases.

Account Type	RecTrac WebXPress CCard Device Setting	PlugNPay Setting	PlugNPay Settlement Result
Regular Retail	Automatic	Yes/Automatic	Automatic
	Manual	Yes/Automatic	Automatic
	Automatic	***No/Manual***	***Automatic***
	Manual	No/Manual	Manual

Tip Processing	***Manual***	***No/Manual***	***Manual***
WebTrac	***N/A***	***No/Manual***	***Depends***

VSI-Recommended Settlement Options Explanation

The VSI-recommended settings in the table above appear in ***italics***. A full explanation appears below.

Regular Retail: Each credit card transaction that is authorized will be settled automatically by PlugNPay when they run their settlement sweep.

Tip Processing: Authorization will occur when the patron's credit card is swiped for the amount of the sale *before* the tip is added. Settlement occurs *after* the tip is added to the initial transaction and must be initiated through RecTrac. *For Example: A patron's food bill comes to $100. When you swipe the card, PlugNPay authorizes a $100 sale. The patron leaves a $20 tip. You add the tip to the transaction using the Tip Processing Program. When you settle the credit cards, the transaction goes to PlugNPay as a $100 + $20 transaction.*

WebTrac: Depends: When the PlugNPay settlement option is set to 'No/Manual,' settlement will NOT occur until RecTrac "marks" the transaction for settlement. RecTrac "marks" the transaction as ready for settlement when the patron is returned to WebTrac from the PlugNPay site. Transactions "marked" for settlement will be settled when PlugNPay runs their settlement sweep.

RecTrac WebXPress Credit Card Device Manual Settlement Option

If you selected to settle batches manually using the Credit Card Terminal, you will need to perform the following set of steps at the end of each day. To use this option, change the **Settlement Type** field in the PlugNPay WebXPress device to **Manual**.

Your account type can be set to either Retail or Restaurant. However, VSI strongly recommends you use this option if you have a Restaurant account credit card device and use Tip Processing.

1 Run the Tip Processing program to add tips to your transactions, if necessary.

2 Go to Daily Processing • System • Credit Card Processing • Credit Card Terminal.

3 Highlight the merchant(s) for which you wish to manual-settle transactions.

4 Click the down arrow next to the **Action Type** field and select **Perform Settlement** from the drop down list.

5 Enter the range of transaction dates for which you wish to auto-settle transactions.

OR

Press the **F9** key or right-click from within the fields to select the appropriate dates from the calendar.

6 Enter the range of transaction times for which you wish to auto-settle transactions. Note that all transactions in the batch for the selected merchant, date, and time ranges will be listed in the browser box at the bottom of the screen.

7 Click **Continue**. The following question will appear: *All Unsettled Transactions For Selected Merchants Above Will Be Settled. Are You Sure You Want To Continue?* Click **Yes.**

Reporting on Credit Card Transactions in RecTrac

1 Go to Reports • System • Credit Card Reports • Credit Card Report.

2 Highlight the Merchant(s) in the **Available Merchants** browser box on which you wish to report.

> **Note:** The Merchant(s) that appear in this browser are dependent upon the Merchant ID linked to the PlugNPay device linked to your user ID as well as all merchant IDs listed in the **Users Linked to this Device…** field on the PLUGNPAY Device Other Settings screen.

3 Select whether you want to print information on transactions originating from **Payment Programs** (RecTrac), the **PlugNPay Terminal**, or **Both**.

> **Note:** If you want to check your RecTrac Cash Journal and GL Distribution Report against this report, you should select RecTrac as the option in this field. Otherwise, if you processed any blind sales or credits using the PlugNPay Terminal program, your Cash Journal and GL Distribution Report will not balance when checked against this report.

4 Select whether you wish to show transactions with a status of: **Authorized**, **Settled**, **No Capture**, **Voided**, **Failed**, or **Declined**.

5 Fill in all remaining report selection criteria based on the data that you want to view on the report.

6 Click **Print**. You will continue to the Print Option Selection screen. Click **Print** or **Preview**.

Querying Transactions on the PlugNPay Website

The Transaction Administration area of the PlugNPay website allows you to query transactions based on the processing date as opposed to the settlement date.

1. Go to https://pay1.plugnpay.com/admin
2. Log into your PlugNPay account.
3. Click **Transaction Administration**.
4. Enter a beginning and ending date range. For best results, allow at least a day between dates (i.e. 02/24/2010 – 02/25/2010).
5. Determine you Submitted Date setting.
    - If Disabled/Off – The query will pull transactions that were processed and/or settled over the complete date range. *For Example: Your date range is 2/24 – 2/25. Running the query with the toggle off will pull all transactions process or settled on 2/24 as well as any transactions that were processed on 2/24 but settled on 2/25.*
    - If Enabled/On – The query will pull transactions that were processed on those dates only. It will not pull transactions that were settled.
6. Click **Submit Query**.

Perform Test Transactions in WebTrac

Perform the following steps only if your organization uses WebTrac.

Prior to going live with PlugNPay ERI, VSI strongly recommends you perform two (2) test ERI transactions on your WebTrac Transaction server, one using RecTrac GUI and the other using WebTrac.

The following steps will walk you through the process:

1. Log into RecTrac as the WebTrac user (typically userid 'WWW').
2. Perform an ERI test transaction in GUI.
3. Remain on the Transaction server and log into WebTrac with a valid account (i.e. do NOT sign in as "Guest.").
4. Perform an ERI test transaction as a WebTrac customer.
5. Watch the WebTrac transaction carefully and ENSURE you see the "Please Wait" images (and not a blank screen) as the transaction processes.
    - IF you see the "Please Wait" image, continue through steps 6 – 15 below.
    - IF you do NOT see the "Please Wait" image, continue through steps 6 – 15 below but be sure to add the "Please Wait" image when done.

6 Log into your PlugNPay account and review the transactions. They should look identical, with an Auth and a PostAuth for each payment.

7 IF the transactions are identical, you are done.
IF the transactions are NOT identical (if you do not see a PostAuth for the WebTrac transaction), proceed to step 8.

8 Ensure that your firewall is open on port 443 between the Transaction server IP address and the PlugNPay urls on your WebXPress Credit Card device. See also: Transactions Not Authorized below.

9 Ensure that the Windows User account you are using to log into the Transaction server is the same Windows Users account you used when installing Progress on that workstation.

10 Ensure that your OpenEdge 10.1 admin service is using the same account from step 9.

- Go to Start • Settings • Control Panel.
- Double-click on **Administrative Tools**.
- Double-click on **Services**.
- Right-click on AdminService for OpenEdge and select **Properties.**
- Click the **Log On** tab and ensure you are set to:
    - *Local System Account*– if using this option, ensure the Local Host is a Window Admin account
    - *This Account* – if using this option, ensure that your Domain Administrator Account is being used.
- Click **OK** and exit Administrative Tools

11 Register the winhttp.dll, which is located in c:\windows\system32

- Go to Start • Run
- Change directories to c:\windows\system32
- Type the following: *Regsvr32 winhttp.dll*
- You should receive a message indicating the .dll was registered successfully.
- Exit the Command Prompt.

12 Ensure that the Progress Admin username (the username being used by Progress Admin Service) has full rights to the winhttp.dll

- **Open Windows Explorer**
- **Browse to C:\Windows\system32**
- **Scroll to and right-click on *winhttp.dll***
- **Right-click and select Properties • Security.**
- **Review the user IDs in the Group or usernames field and ensure the username being used by Progress Admin Service is listed in the box and has full rights.**
- **Take appropriate action (add user, if necessary, or click Cancel if the user exists)**
- **Exit back to the desktop when done.**

13 Log back into WebTrac using a valid user account (do NOT log in as 'Guest') and process another transaction.

14 Log into PlugNPay and ensure you have an Auth and PostAuth record.

15 Contact VSI Support (877-883-8757) if you still do not have a PostAuth record.

Adding a "Please Wait" Image to your WebTrac transactions.

Complete these steps only if you did NOT see a "Please Wait" image when processing your test transaction in WebTrac (steps 4 – 5 above).

The following steps will add a "Please Wait" image to replace the blank screens your customers see when using certain processes in WebTrac. The "Please Wait" image should keep customers from hitting the back/refresh button multiple times at the blank screen.

1 Overwrite or append these new Tags to the bottom of the WebTrac style sheet on your web server. VSI default style sheets are stored in the \wbstyles folder on your web server. Custom style sheets may be located there or in a sub-folder within \wbstyles

```
#cover {
background-color: #FFFFFF;
background: #FFFFFF;
position: absolute;
z-index: 1998;
filter:alpha (opacity=90);
-moz-opacity: 0.9;
left: 0px;
top: 0px;
width: 100%;
height: 100%;
}

#plswait {
clear:both;
font-weight: bold;
z-index: 1999;
position: absolute;
top: 35%;
left: 35%;
}
```

2 Copy the following image to the \wbimages folder on your web server. This image is stored on the Vermont Systems FTP site: *pleasewait.gif* On the FTP site, browse to: \File Updates And Drivers\WebServer\102\wbimages

3. Overwrite the following file to the \wbjavascripts folder on your web server. This file is stored on the Vermont Systems FTP site: *vsijava.js* On the FTP site, browse to: \File Updates And Drivers\WebServer\102\wbjavascripts
4. Stop and start your web brokers.
5. If you are using custom language codes, remember to make the same changes in the \<LANG> subfolders under each of the above directories, where <LANG> is the name of your Language Subfolder (*For example: \CUSTOM, \POOL, \GOLF, etc…)*.

Using a Proxy Server to Access the Internet for PlugNPay

Perform the following steps only if your organization uses a Proxy Server to access the Internet.

Proxy servers have the potential to cause communication issues with the queries between RecTrac and Plug'nPay. VSI recommends performing the following steps on your PlugNPay point of sale workstations.

Windows 7 / Vista Operating Systems

1. Login to the machine with local administrator privileges.
2. Go to Start • Run • cmd.
3. Type *netsh* and press the <Enter> key.
4. Type *winhttp import proxy source =ie* and press the <Enter> key. This command imports the proxy settings in the Internet Explorer Web browser's Internet Options.
5. Type *Exit* to quit the netsh utility.
6. Type *Exit* to quit the cmd utility.
7. Restart the workstation.

Windows XP Operating Systems

1. Login to the machine with local administrator privileges.
2. Go to Start • Run • cmd.
3. Type *proxycfg.exe –u* and press <Enter> key. This command will allow WinHTTP to use the proxy settings already defined in IE.

   If you have multiple proxy servers, type

proxycfg – p "IP address 1 IP address 2:port number" "bypass list and press the <Enter> key.

4. Type *Exit* to quit the cmd utility.
5. Restart the workstation.

Troubleshooting

Explanation of “Record Not Found” Message

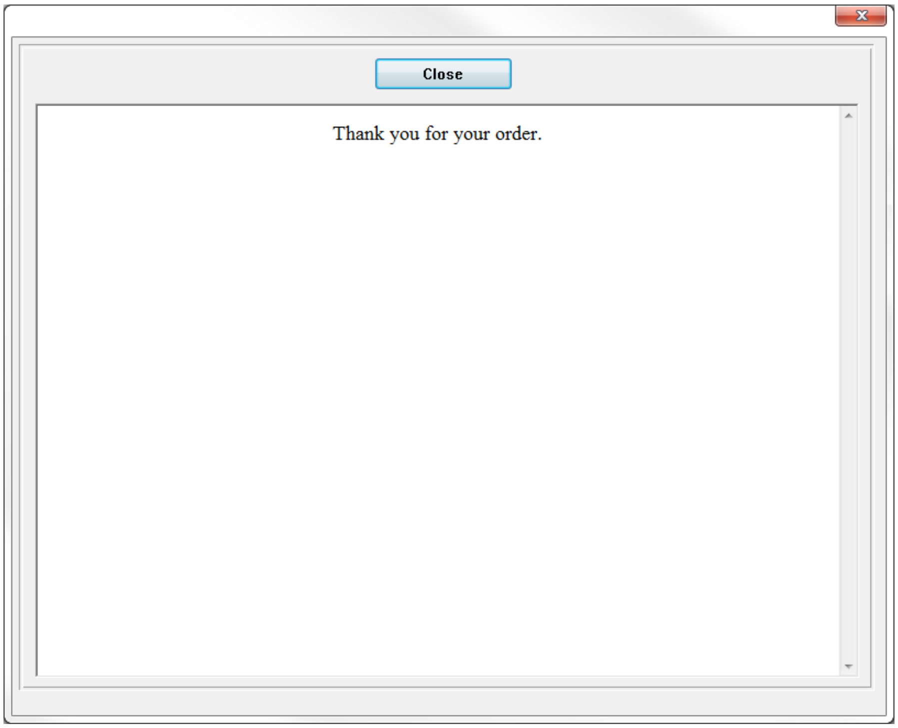
When a credit card payment is processed in RecTrac, the Card Processing screen below appears. This screen is a combination of a RecTrac program/screen and Plug n’ Pay (PnP) transaction page. RecTrac is acting, as a web browser and simply displaying the PnP transaction page. The following occurs when credit card processing is initiated:

RecTrac creates a unique Order ID and sends it to Plug n’ Pay (PnP) when their Transaction Page is opened. The Order ID is used to link the transaction on the PnP server to the transaction in RecTrac.

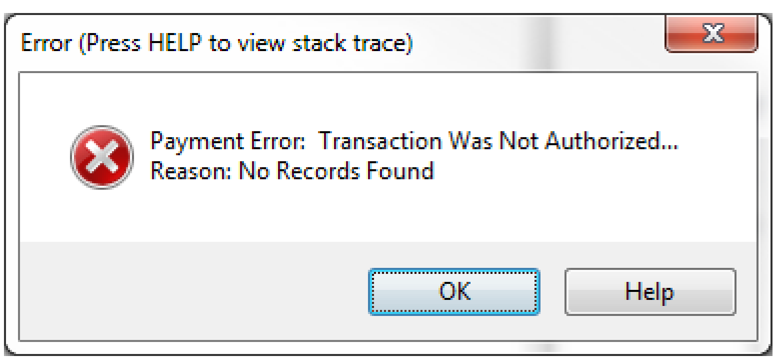
RecTrac / Plug n’ Pay Card Processing Screen:

Until the **Close** button is clicked, all processing is occurring on PnP's transaction web page (the middle of the page). At this point, standard procedure is to swipe a credit card then click **OK** (or anywhere else in the PnP web page area) to populate the Name, Credit Card #, and Exp date fields below.

When you click the **Summarize Payment** button, PnP authorizes the credit card via their web site. RecTrac is not accessed or updated in any way. Notice that once the transaction processes, their website changes, but the RecTrac portion remains unchanged.



The **Close** button signals RecTrac to query the PnP server for the results of the current Order ID. Prior to clicking **Close**, no credit card transaction results are communicated from PnP to RecTrac. If the transaction was successfully processed and the Order ID is found on the PnP side, the sale is good in RecTrac, a regular receipt and credit card authorization receipt is generated, etc. If the Order ID is not found you will receive the message below:



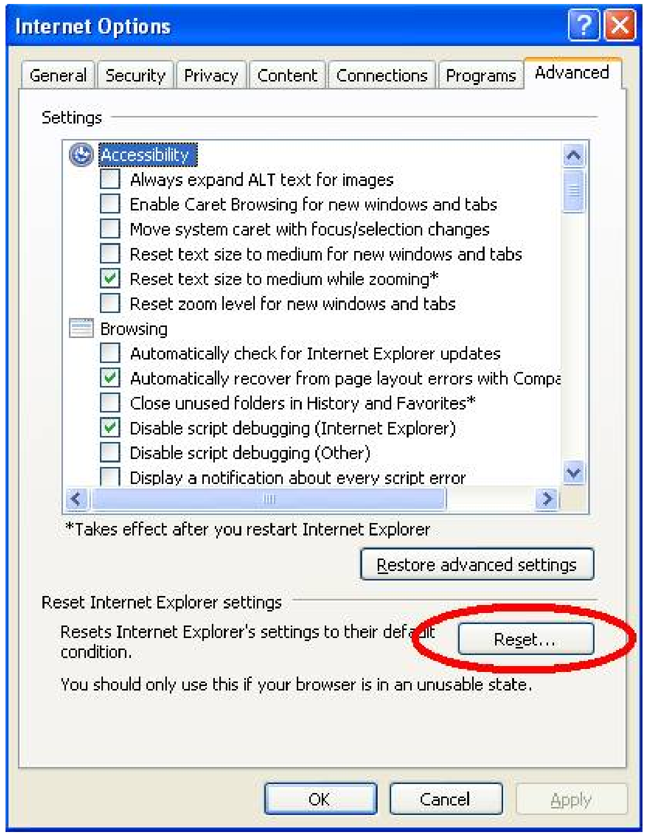
This means that when RecTrac checked the transaction status on the PnP side, it was unable to find the sale on PnP's server. There are two reasons this could happen:

1. At the time of the transaction, RecTrac was searching for the transaction on the PnP side before the card was finished processing. If the clerk is waiting for the message "Thank you for your order", this should never happen. However, if the clerk clicks **Close**, then clicks **Summarize Payment** before the above message displays, a problem results. In order to help solve this problem, we added a query pause and number of retries to the PnP device in RecTrac to delay RecTrac from checking for the transaction too early. However, this is not a perfect solution, as there is no way to know how long it could take for the sale to process on PnP's side. The safest decision is to always wait for the "**Thank you for your order"** message.
2. The transaction was not processed completely prior to clicking the **Close** button, thus it will not be found on the PnP server. So, clicking the **Close** button before clicking the **Summarize Payment** button will cause this error to occur.

General Card Swipe Issues

If you find your credit card swipers are not functioning properly verify the following:

1. Verify the clerk is waiting log enough for the entire credit card data to populate in the swipe field. The cursor should be blinking steadily at the end of the field.
2. Be sure the machine is running Internet Explorer 7 or higher.
3. PS2 card readers do NOT function with PlugNPay.
4. Add https://pay1.plugnpay.com/ as a trusted site on all workstation IE browsers.
5. Reset the Internet Explorer advanced settings. This is under Tools • Internet Options • Advanced Tab • Click **Reset**.



6 Enter the following URL into a web browser:

https://pay1.plugnpay.com/payment/pay.cgi?publisher-name=xxxxxxxxxxx&paymethod=swipe&askamtflg=1

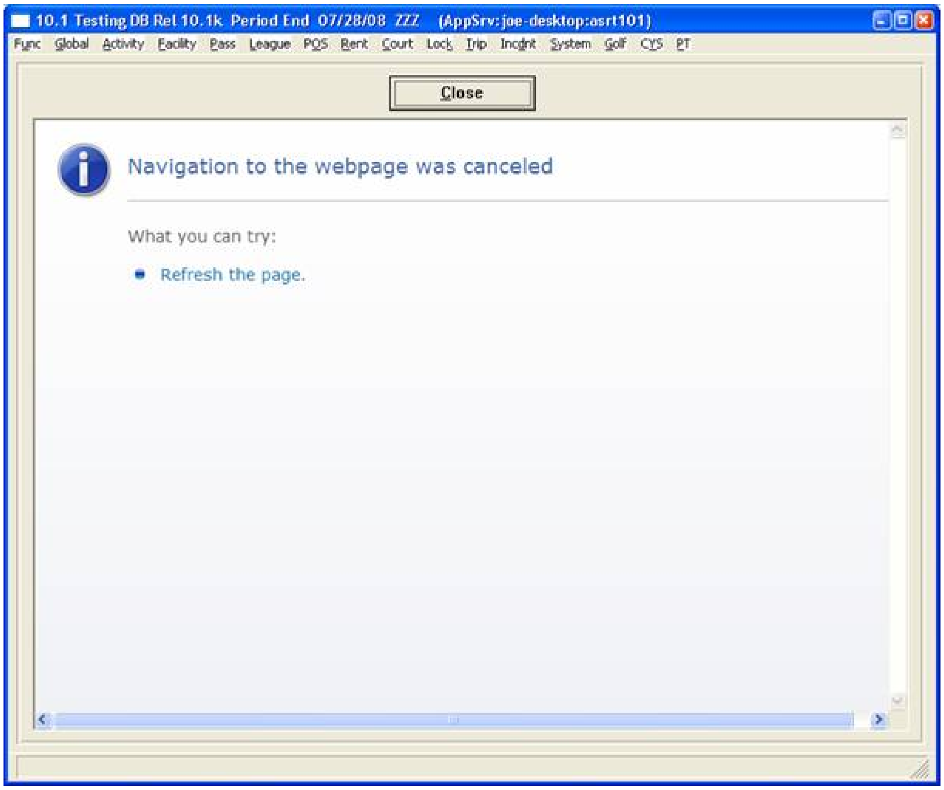
where xxxxxxxxxxxxxx is your PlugNPay username. This can verify that the same problem exists outside RecTrac.

7 If you are having trouble swiping and are using a regular MSR keyboard wedge type reader, swipe a credit card in the Notepad editor and make sure both tracks are on the same line. If there is a carriage return between the tracks, this means the card reader is not configured properly and therefore will not swipe in RecTrac.

PlugNPay Portal is Inaccessible

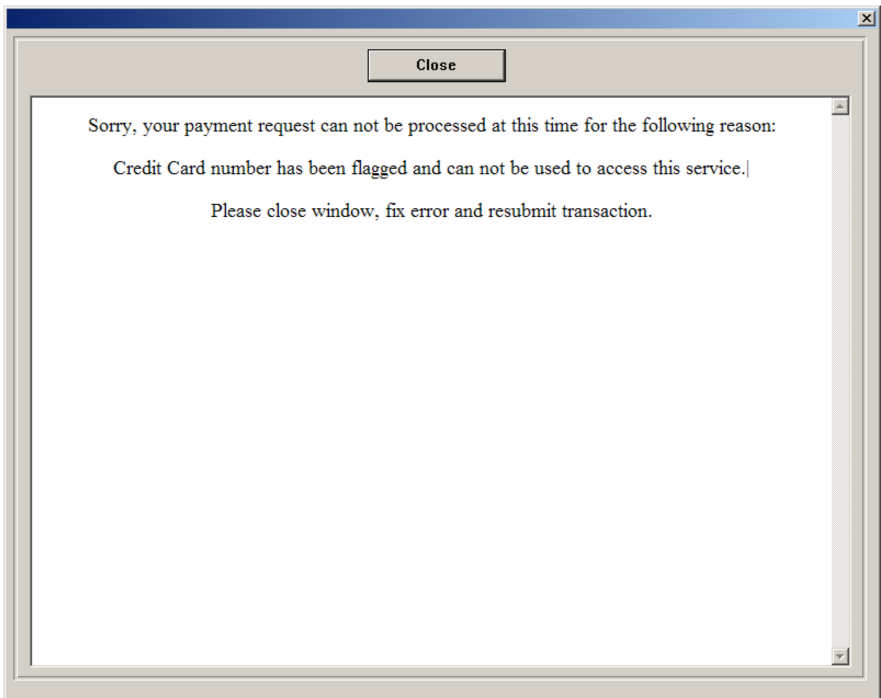
You will receive the following message if the PlugNPay portal cannot be accessed during a credit card sale. The most common reason is internet failure. Check your connections and ensure your network is operational by various means, such as attempting to hit another website.

If your network is operational and if you have connectivity to the World Wide Web and still get this message, contact PlugNPay at (800) 945-2538 for further assistance.



Card Failure Messages from PlugNPay

The PlugNPay portal will return failure messages for various reasons, such as invalid cards, declines and etc… In those instances, the portal will generate messages such as the one below, which indicates a 'flagged' card that PlugNPay will not process.



Exceeding the Transactions Allowed per Hour Threshold

A similar message may appear from the PlugNPay portal if you exceed the threshold number of transactions allowed per hour. In that event, you should login to your PlugNPay account and disable FraudTrack as outlined above.

Transactions Not Authorized

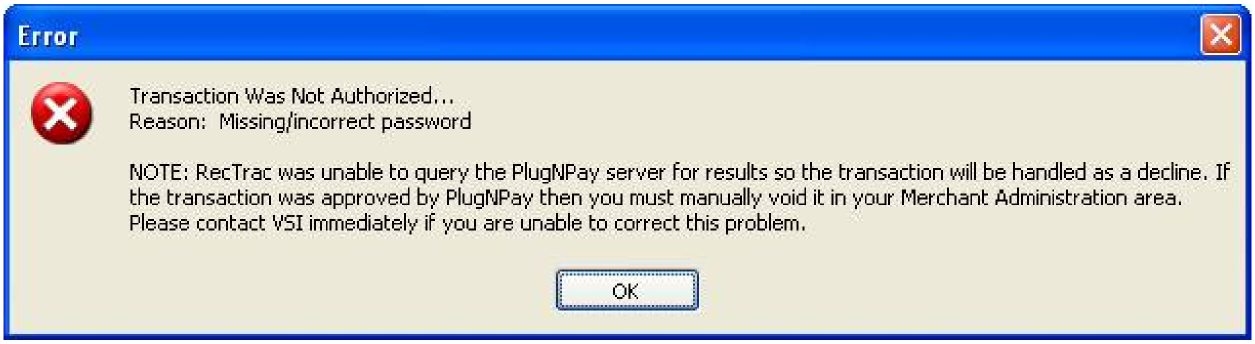
PlugNPay will NOT authorize transactions if:

- **The password on your Express Credit Card device is missing or invalid.**
- **Your IP Address has not been registered on the PlugNPay website.**

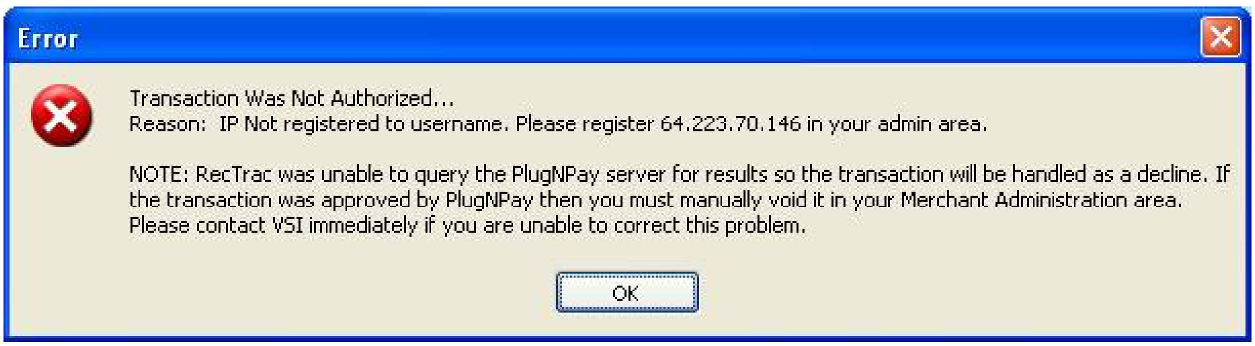
Users running RecTrac 10.1l or 10.1m have only ONE indicator if either of the above is true: They will NOT be taken to the 'Thank You for Your Order' screen but will instead be brought back to RecTrac. PlugNPay does not indicate the cause of the transaction failure.

Users running RecTrac 10.1n (or later) will receive Transaction Not Authorized messages from RecTrac in the event one (or both) of the above is true.

Invalid or Missing Password on the WebXPress Device



IP Not Registered with PlugNPay



Transactions Not Authorized Through Port 443

VSI recommends you open port 443 fully for incoming and outgoing traffic.

However, if you place an IP filter on your system to only allow connections from certain IP addresses through port 443, make sure the following IP addresses are allowed access via the firewall and any proxy servers.

Server IPs:

- 69.18.198.4 – PlugNPay's payment host IP for traffic outbound from their network. You need to allow inbound traffic on port 443.

- 69.18.198.21 – PlugNPay's payment host for traffic inbound to their network. You need to allow outbound traffic on port 443.
- 96.56.10.14 – This is the PlugNPay off IP and would be used ONLY if PlugNPay initiated desktop assistance from their office to you.

The above IP addresses belong to and are used by PlugNPay. Their servers and office workstations use these IP addresses. Setting up your system to allow access from these IP addresses will prevent transaction not authorized failures as PlugNPay add/move servers and/or extend their system's abilities.

> **Note:** Optionally you can authorize inbound/outbound traffic to these addresses using port 80 as well. Be aware that port 80 is NOT secure. VSI recommends using these ports ONLY if you do not have SSL Certificates for ERI Credit Card processing. Contact VSI for further details, if needed.

Require IP Match

The PlugNPay Security Administration Area contains a toggle setting to *Require Match* for IP Addresses. When enabled, transactions will be allowed from the specific IP Addresses listed on that browser ONLY.

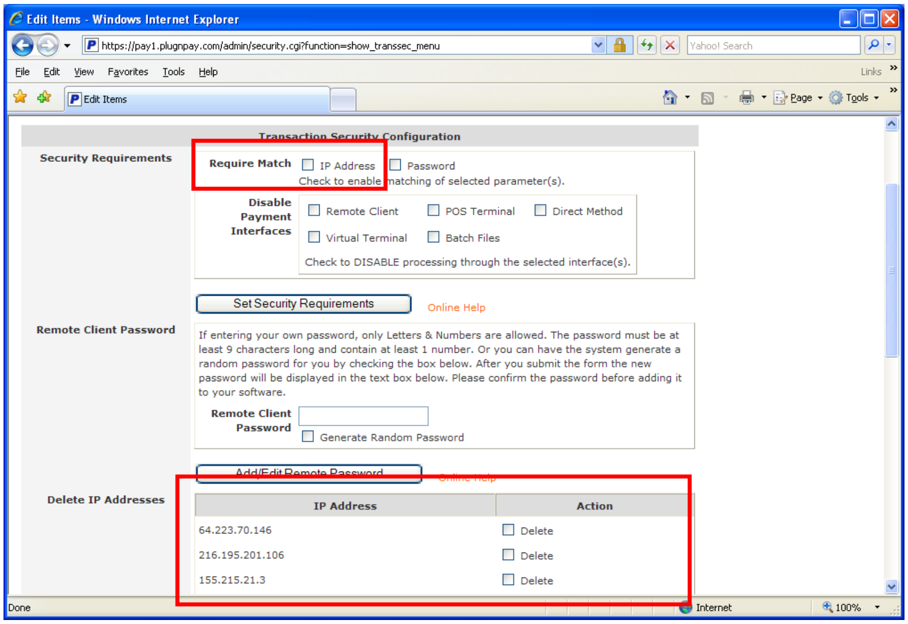
VSI highly recommends DISABLING this option for GUI-only processing.

IF you use WebTrac, this option MUST be disabled or else your patrons will not be able to purchase your products via the web.

> **Note**: Regardless if you disable the Require IP match for your WebTrac account, transactions may not get the proper Post Authorization, UNLESS you register the IP address(s) of your Transaction server.

To Review/Change Your Current Setting:

1. Go to: **https://pay1.plugnpay.com/admin/**
2. Using the Login and Password given to you by PlugNPay, log into your account.
3. Under *Settings*, click **Security Administration**.
4. On the Security Administration Area screen, click **Transaction Security Configuration**.
5. IF you process sales via GUI only, VSI recommends disabling the *Require Match* for IP Address toggle.
   IF you use WebTrac, ENSURE the *Require Match* for IP Address toggle is deselected.
6. Scroll down the page and review the IP Addresses currently listed. IF you enabled the toggle in step 5, transactions will be allowed from the IP Addresses listed here ONLY.



7 To add additional IP Addresses, click **Add IP Address**. Refer to [Account Setup for Using the PlugNPay Website]() above for further information.

8 Close the window by clicking the ‘x’ in the upper right-hand corner of the screen and log out of the PlugNPay site.

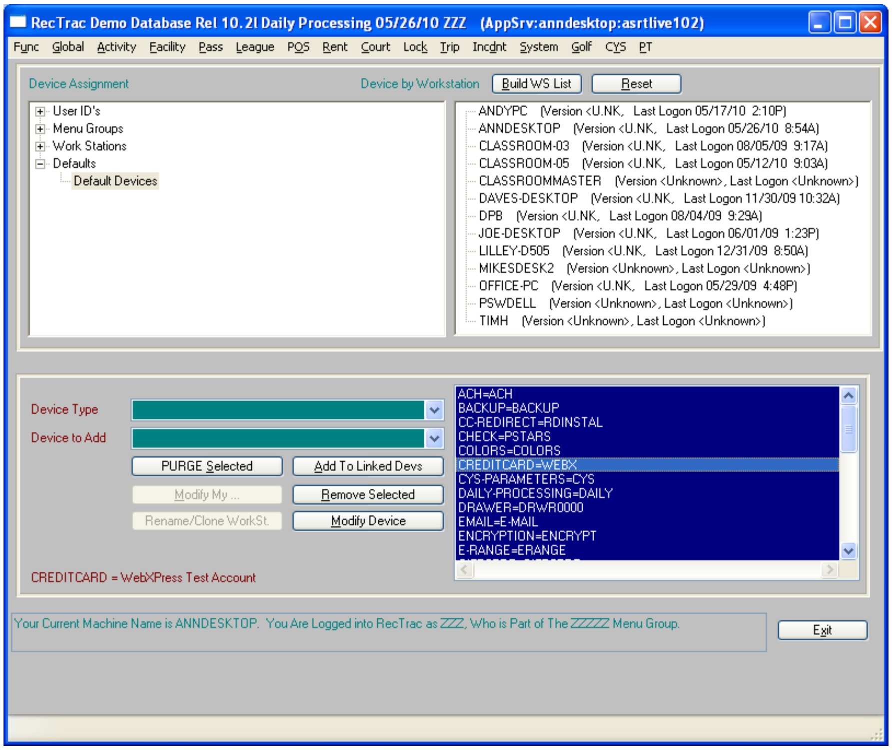
Using File-Drop Method for Authorizations

The File-Drop method can be used as an alternative to direct credit card authorizations, requiring a shorter Internet connection time than direct authorizations. To use this option, you must notify PlugNPay for your account to be setup accordingly. For more information regarding this process contact VSI Customer Support.

> **Note**: This option is available for customers running RecTrac 10.2L or higher, and is available for RecTrac (GUI) ONLY. You CANNOT use this feature for your WebTrac credit card device/PlugNPay account.

1 Go to: File Maintenance • System • Device Maintenance • Device Assignments.

2 Using the Device Assignment hierarchy click the ‘+’ next to level to which your PlugNPay device is linked. In the example shown below our credit card device is linked at the Defaults level.



3 Highlight the device and click **Modify Device**.

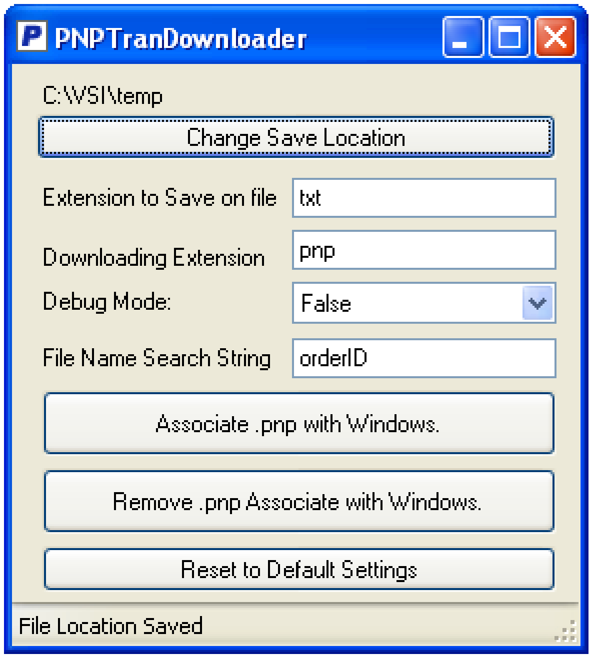
4 Choose the '*Use File Method for Results*' option.

5 Click **Done.** If you have multiple PlugNPay accounts, repeat steps 2-5 until all of your RecTrac (GUI) credit card accounts have been modified.

6 When you have modified all of the appropriate credit card devices click **Exit**.

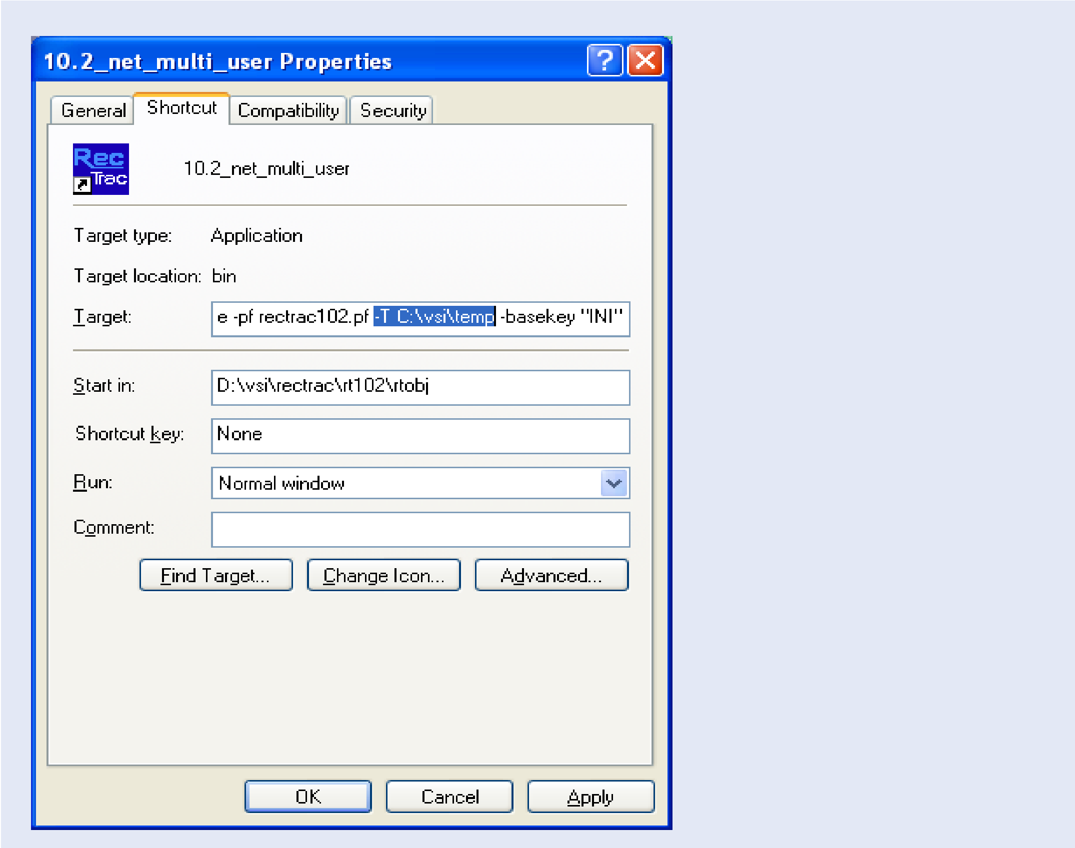
7 Now using *My Computer* or Windows Explorer, you will need to browse out to ***x:\vsi\rectrac\misc***, where x:\ is the drive that RecTrac has been installed.

8 Locate the PNP Transaction Downloader.exe file and double-click on it. You will receive a message box that looks like the this:



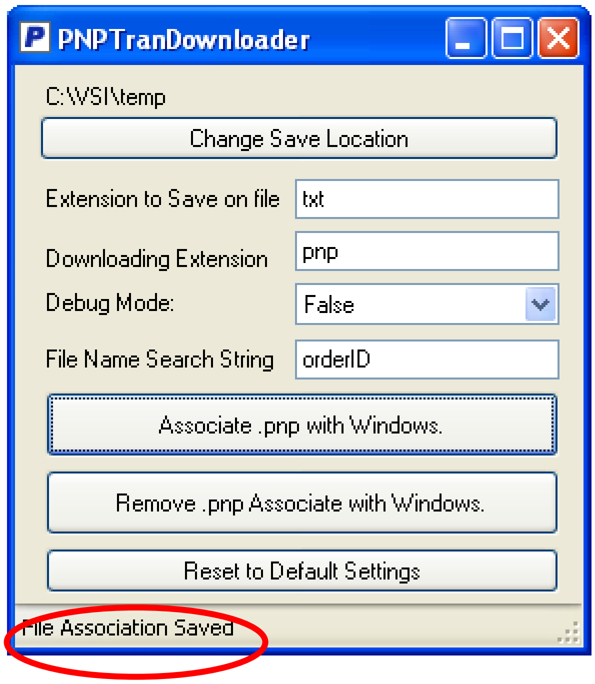
9 First, click the **Change Save Location** button and browse to your local temporary directory. This is the directory where the raw response data will be stored in the form of a .txt file. The .txt file will be deleted as soon as the transaction has been processed and the clerk clicks **Close**.

> **Note**: This location must match your –T parameter (temporary directory) – typically x:\vsi\temp, where x:\ is the drive that RecTrac has been installed. Right-click on your RecTrac icon to find the –T parameter on the Target line.



10 Click **OK**.

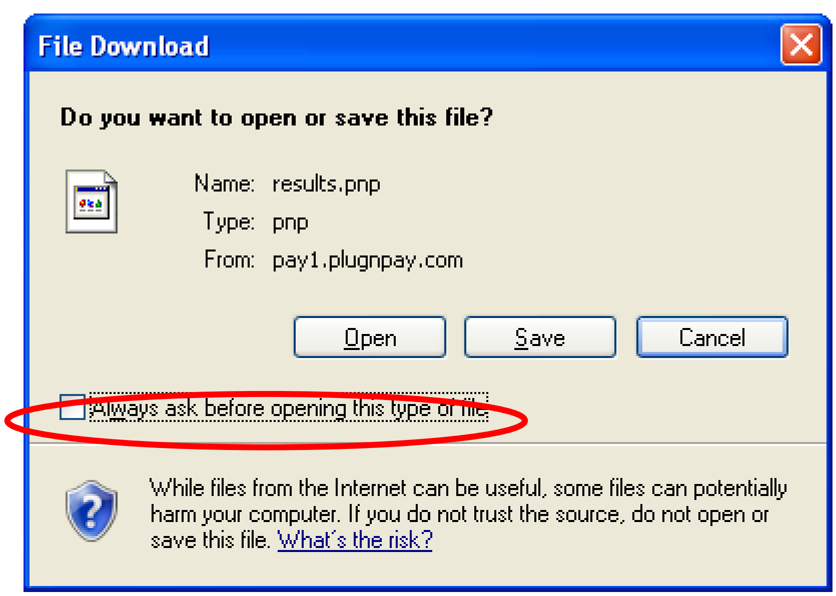
11 Change the remaining fields to reflect that of the screen-shot shown above and then click **Associate .pnp with Windows**. The message in the lower left-hand side of the message box should now say **File Association Saved**.



12 Click the red box in the upper right-hand corner of the message box to close the window.

The First Transaction Processed Using this Feature

Important Note! When you process the first transaction after enabling this feature you will receive the message box shown below. DE-SELECT the ***Always ask before opening this type of file*** option and click **Open**. Click **Close** once the transaction has finished processing.



If PlugNPay Resets Your Administrator Password

At its discretion, PlugNPay may determine that Administrator Passwords need to be reset for all of their clients. In this event, PlugNPay will email to advise you of the reset and invite you to log onto their site and reset your password. The email from PlugNPay will include a temporary password with which to log onto their site.

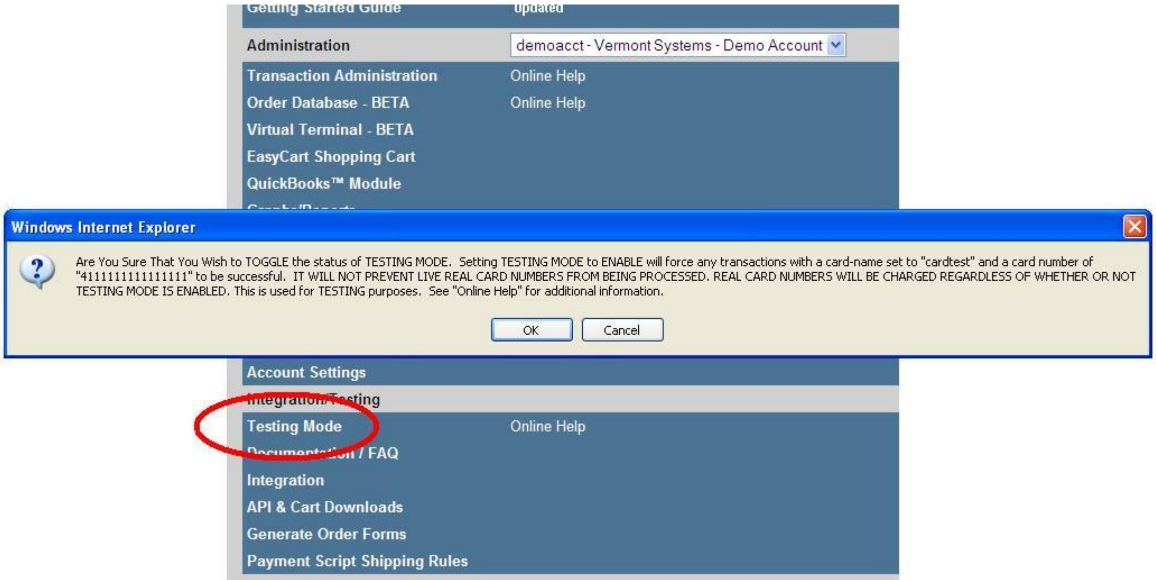
To change your Administrator Password once you have received the email and temporary password from PlugNPay:

1. Login to the PNP administration area, https://pay1.plugnpay.com, with the new temporary password you received.
2. You will be prompted to create a new password. This new password can be used to access your PNP administration area.

Note: If you are using Remote Client Password, your processing should not be affected if/when PlugNPay opts to reset your Admin Password. Regardless, you should always follow the steps above if/when PlugNPay resets your Admin Password.

Testing Mode

Warning! If you selected the option on the PlugNPay website to process in **"Testing Mode,"** be advised that regular credit cards can still be processed and charged. This option is intended only for using a demo credit card number. Contact VSI Support for the demo card number, if needed.


Administration
demoacct - Vermont Systems - Demo Account
Transaction Administration
Online Help
Order Database - BETA
Online Help
Virtual Terminal - BETA
EasyCart Shopping Cart
QuickBooks™ Module
Windows Internet Explorer
Are You Sure That You Wish to TOGGLE the status of TESTING MODE. Setting TESTING MODE to ENABLE will force any transactions with a card-name set to "cardtest" and a card number of "4111111111111111" to be successful. IT WILL NOT PREVENT LIVE REAL CARD NUMBERS FROM BEING PROCESSED. REAL CARD NUMBERS WILL BE CHARGED REGARDLESS OF WHETHER OR NOT TESTING MODE IS ENABLED. This is used for TESTING purposes. See "Online Help" for additional information.
OK
Cancel
Account Settings
Testing Mode
Online Help
Integration
API & Cart Downloads
Generate Order Forms
Payment Script Shipping Rules

Charging Convenience Fees

To help offset the “cost of doing business” and in lieu of raising prices across the board, many municipal organizations charge their customers convenience fees which are usually determined either by where (online or in the store, for example) or how (method of payment, for example) a customer shops.

Charging convenience fees for the use of credit cards can be a superior solution to raising overall prices because it passes along the aforementioned “cost of doing business” to those most directly responsible for the increased operating costs (the credit card users) while sparing those who utilize other methods of remittance (cash, checks, gift certificates, etc…) any added expense.

You can charge convenience fees using PlugNPay with little additional set up in RecTrac. However, set up is required with PlugNPay to establish and charge convenience fees. The following steps outline the processes required and also offer some considerations prior to establishing convenience fees.

> **Note:** VSI customers using WebTrac can charge convenience fees to their patrons who make purchases over the web. Processing limitations disallow charging convenience fees in RecTrac via GUI (Graphical User Interface) and we therefore offer the following solution through PlugNPay. For consistency, *if* you charge convenience fees through WebTrac and *if* you wish to charge convenience fees for purchases made via GUI, VSI recommends adopting the same solution for both methods.

Convenience Fees Are Charged Outside of RecTrac

First and foremost: when contracting with PlugNPay to charge convenience fees in RecTrac to your customers, be aware that <u>*NO*</u> record of the additional fee <u>*WILL EVER*</u> appear in RecTrac. Convenience fees are completely separate from the RecTrac application and you will not see them on receipts, cash journals, GL reports or any other report or inquiry found in RecTrac.

Convenience fees are between you, PlugNPay and your bank only. A line item for “Convenience Fee” will appear on the PlugNPay web browser after you click **Print** in RecTrac and send the transaction to PlugNPay. Furthermore, your customers will see them reflected on their credit card statements as a separate line item.

For Example: You charge a flat rate $1.00 convenience fee for any purchase over $10.00 made using Credit Cards. You charge $25.00/activity. A patron who signs up for two (2) activities will be charged $50.00 in RecTrac (2x25=50). When the transaction gets sent to PlugNPay, the patron will be charged $51.00 ($50.00 for the enrollments + $1.00 for the over $10.00 purchase). When the *receipt prints from RecTrac, the customer will see ONLY the $50.00 charged. The customer will NOT see the additional $1.00 convenience fee charge. When you settle your credit cards for the day against RecTrac, you will have to account for the $50.00 only because the $1.00 convenience fee is contracted between you, PlugNPay and your bank and will take place on a separate merchant account. When the customer receives his/her credit card statement, two (2) line items for the purchase will appear: One for $50.00 to you for the enrollment and one for $1.00 to you as a Convenience Fee.*

Include Convenience Fee Verbiage on Your Daily Comment Codes in RecTrac

Since your customers will not see convenience fees on the receipts generated through RecTrac, VSI advises you to update your Daily Comment Codes in RecTrac to reflect your convenience fee policy. When linked to the proper modules on your Receipt Format device(s), Daily Comment Codes will print with every receipt generated. In this manner you can use RecTrac to inform your customers that, depending on their method of payment, an extra fee may be incurred and you can give them the equation for how it is calculated, if desired.

To Update Daily Comment Codes

- Daily Comment Codes are managed in Comment Code Maintenance (File Maintenance • System • Other Maintenance • Comment Code Maintenance).
- To print Daily Comment Codes on your receipts, link them to the appropriate module on the Custom Receipts screen of your Receipt Format Device (File Maintenance • System • Device Maintenance).

Convenience Fee Calculation and Sub-Merchant Accounts

To set up and charge convenience fees you will have to contact PlugNPay to acquire sub-merchant accounts for each primary merchant account from which you want to charge convenience fees. Once in contact with them, you can discuss options for how you wish to calculate the convenience fees.

Sub-Merchant Accounts

To process convenience fees, you will have to setup a sub- merchant account for each primary merchant account from which you wish to charge the fees. The primary account will have no convenience fees linked to it, so the deposit from that account will always match your RecTrac Cash Journal for credit cards. The sub-merchant account will be between PlugNPay, you and your bank and it will constitute 100% of your convenience fees.

Contact PlugNPay if you have additional questions on Convenience Fee sub-merchant accounts.

Convenience Fees Calculation

PlugNPay allows for flat rate and/or percentage based convenience fees. The purchase amount is broken down into “buckets” (aka dollar amount thresholds) and each bucket is assigned a flat rate, a percentage rate or a combination of both as determined by you. The following example displays one solution only (flat rate + percentage), but be aware that PlugNPay is flexible and that you can have as many buckets as needed.

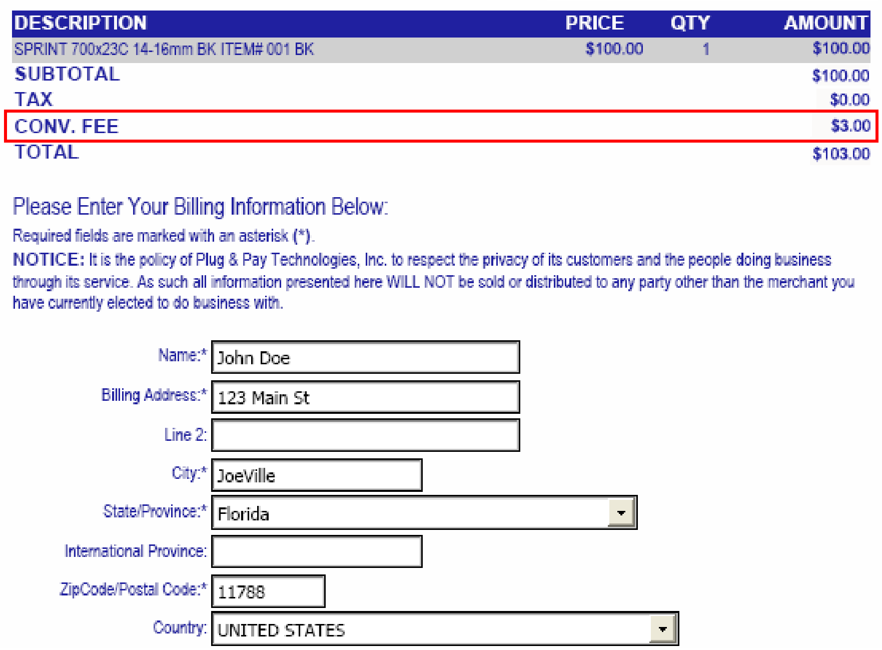
You specify two (2) buckets (aka dollar amount thresholds). The first bucket applies a flat rate amount of $1.00 to any purchases totaling $0.01 - $50.00. The second bucket applies a 2% rate to any purchase of $50.01 or more. The purchase amount = $100.00. The convenience fee = $3.00 ($1.00 flat rate (bucket 1) + 2% of $100.00 (bucket 2, $2.00) = $3.00). The total reflected in RecTrac = $100.00. The total reflected on the customer Credit Card statement = $103.00 (one line item for $100.00 and another for $3.00).

Known Limitation

At present, PlugNPay cannot differentiate convenience fees based on Credit Card type/brand. VSI will contact you in the event this changes.

Convenience Fees on the PlugNPay Website

Using the calculation from the example above, the following screen shots display how convenience fees will be reflected on the PlugNPay Website, once a RecTrac Credit Card transaction is transferred there.



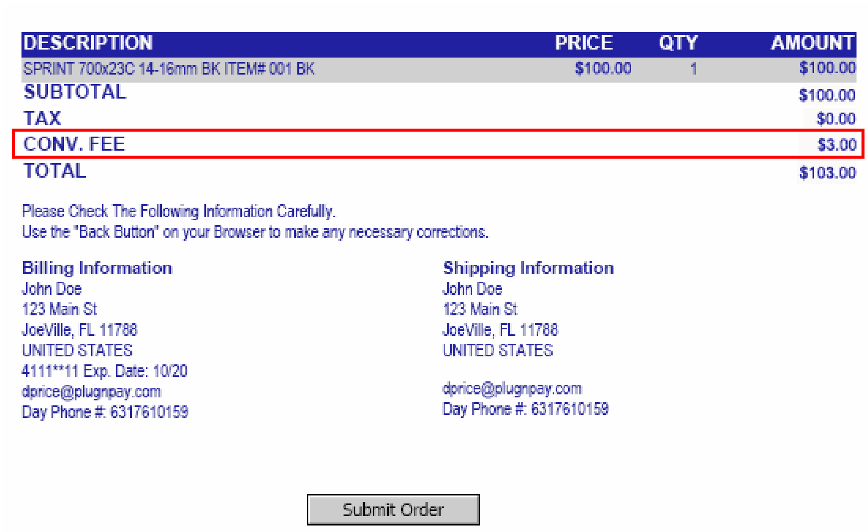
DESCRIPTION	PRICE	QTY	AMOUNT
SPRINT 700x23C 14-16mm BK ITEM# 001 BK	$100.00	1	$100.00
SUBTOTAL			$100.00
TAX			$0.00
CONV. FEE			$3.00
TOTAL			$103.00

Please Enter Your Billing Information Below:

Required fields are marked with an asterisk (*).

NOTICE: It is the policy of Plug & Pay Technologies, Inc. to respect the privacy of its customers and the people doing business through its service. As such all information presented here WILL NOT be sold or distributed to any party other than the merchant you have currently elected to do business with.

Name:* John Doe
Billing Address:* 123 Main St
Line 2:
City:* JoeVille
State/Province:* Florida
International Province:
ZipCode/Postal Code:* 11788
Country: UNITED STATES



DESCRIPTION	PRICE	QTY	AMOUNT
SPRINT 700x23C 14-16mm BK ITEM# 001 BK	$100.00	1	$100.00
SUBTOTAL			$100.00
TAX			$0.00
CONV. FEE			$3.00
TOTAL			$103.00

Please Check The Following Information Carefully.
Use the "Back Button" on your Browser to make any necessary corrections.

Billing Information
John Doe
123 Main St
JoeVille, FL 11788
UNITED STATES
4111**11 Exp. Date: 10/20
dprice@plugnpay.com
Day Phone #: 6317610159

Shipping Information
John Doe
123 Main St
JoeVille, FL 11788
UNITED STATES
dprice@plugnpay.com
Day Phone #: 6317610159

Submit Order

Appendix A: MagTek IPAD

Complete the following steps only if you are using the MagTek IPAD pinpad hardware. Perform the following steps on each workstation from which you will process transactions using the MagTek IPAD pinpad.

You must be running RecTrac *10.3L* or greater to use a MagTek IPAD.

Access to the VSI FTP site (ftp://www.vermontsytems.com) is required. Contact VSI support for the current login credentials.

> **Note:** DO NOT plug the MagTek IPAD unit into the workstation until you are instructed to do so.

Product Description

The IPAD is a secure PIN entry device. The IPAD provides end-to-end security solution to prevent personal cardholder data breaches while bringing convenience and speed to Retail and Financial transactions.

The IPAD immediately encrypts data at the point of swipe to safeguard personal information encoded on the magnetic stripe. The encryption takes place within an encapsulated magnetic read head as the card is swiped, eliminating the chance of intercepting clear text data. The data is not in the clear for even a few milliseconds. The IPAD’s data encryption scheme uses the industry standard 3DES algorithm, which offers merchants, processors, issuers, and acquirers the flexibility to manage decryption services themselves or to outsource, thereby avoiding the risk imposed by unproven, proprietary encryption algorithms.

In addition to meeting the requirements established by PCI PED v2.0, the IPAD has MagnePrint®, a proven embedded security feature that authenticates the debit, credit, or gift card and its encoded track data, rendering counterfeit or cloned cards useless. This feature provides a valuable defense to protect the merchant, the acquirer, the processor, the card issuer, and ultimately the consumer.

Unpacking and Handling the MagTek IPAD

Whenever handling the MagTek IPAD, do so with extreme care and caution, being careful not to drop the device. These units are configured with a tamper proof setting that, when tripped, will deactivate the encryption keys and render the unit useless until it is re-injected *by the seller* (i.e. if the encryption keys are deactivated, you will have to return the unit to the vendor and have it re-injected.).

Install the MagTek IPAD Windows Library

Note: DO NOT plug the MagTek IPAD unit into the workstation until you are instructed to do so.

You must be running RecTrac _10.3L_ or greater to use a MagTek IPAD.

1 Log into the workstations using a Windows Administrator account. Open an internet browser and log into the VSI FTP site (ftp://www.vermontsystems.com).

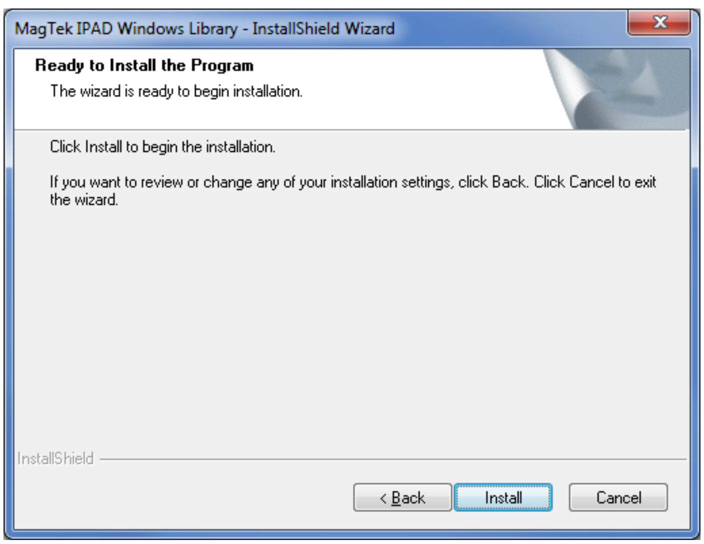
2 On the FTP site, browse to \File Updates and Drivers\MagTek IPAD.

3 Copy the contents of \MagTek IPAD to a temporary directory on your workstation and exit the FTP site.

4 In Windows, browse to the temporary directory to which you copied the contents of \MagTek IPAD. Highlight/select **99510093.exe**.Right-click and choose *Run As Administrator.*

5 At the Open File - Security Warning, click **Run**. At the MagTek IPAD Windows Library - InstallShield Wizard screen, click **Next**.

6 At the Ready to Install the Program screen, click **Install**. Be patient, as this may take a few seconds to begin and complete.



7 Click **Finish** when prompted. You will return to Windows Explorer.

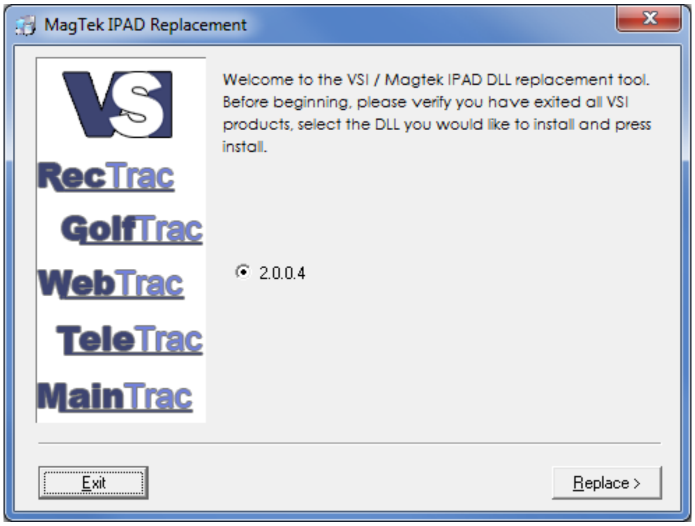
- IF you are installing the MagTek IPAD on a 64-bit workstation, proceed to step 8.
- IF you are installing the MagTek IPAD on a 32-bit workstation, skip to step 12

Note: Complete steps 8 - 11 only if you are installing the MagTek IPAD on a 64-bit workstation.

8 In Windows, browse to the temporary directory to which you copied the contents of \MagTek IPAD. Highlight/select **MAGTEK_IPAD_DLL_REPLACE.exe**. Right-click and choose *Run As Administrator.*

9 At the Open File - Security Warning screen, click **Run**.

10 At the MagTek IPAD Replacement screen, click **Replace>**. Be patient, as this process may take some time to complete.



11 At the MagTek IPAD Replacement - Complete screen, click **Exit**.

12 Exit Windows Explorer and return to your computer desktop.

13 Plug the MagTek IPAD pinpad hardware into an available USB port on the workstation. The unit will install automatically. The LCD will read "Welcome" when the install is complete.

Set Up Your Pinpad Device

Note: If you have an MSR device linked to this workstation in RecTrac, it must be removed.

1 Go to File Maintenance • System • Device Maintenance • Printer/Device Maintenance. Click **Add**.

2 Enter a code for your device, such as 'IPAD.'

3 From the New Type drop down list, select *PinPad*. From the New SubType drop-down list, select *MagTekIPAD*. Click **OK**.

4 Enter a description for your device, such as 'MagTek IPAD device.'

5 Set your *Swipe Pause* value. The Swipe Pause is the number of seconds the PinPad device will allow for a swipe before timing out. VSI recommends a value at/around '15.'

6 Set your *Manual Entry Pause* value. The Manual Entry Pause is the number seconds the device will allow manual input of a credit card number before timing out. VSI recommends a value at/around '60.'

7 Set your *Confirmation Pause* value. The Confirmation Pause is the number seconds the unit will allow for choosing whether the amount being charged is OK. VSI recommends a value at/around '10.'

8 Set your *Display Msg Pause* value. The Display Message Pause is the number of seconds messages, such as 'Approved,' 'Declined,' etc... will display on the LCD. VSI recommends a value at/around '2.'

9 Set your *Buzzer Tone*. The Buzzer Tone value can be numbers 0 - 2. VSI recommends setting '2.'

- 0= No tone.
- 1 = a long tone.
- 2 = two short tones in quick succession.

10 Repeat these steps for each PinPad device you need to create.

11 Click **Next** or **Done** to save your settings. Exit Printer/Device Maintenance and Link the device in Device Hierarchy.

Link the MSR Device in the Device Hierarchy

1 Go to File Maintenance • System • Device Maintenance • Device Assignments.

2 Decide on which level (User, Menu, Workstation, Default) of the Device Hierarchy to link the device. VSI recommends that you link the PinPad device at the workstation level of the hierarchy. If you are unsure of the best level to link a device, please call Vermont Systems Customer Support (1-877-883-8757) for help.

3 Expand the appropriate level and then highlight the appropriate user, menu or workstation

4 In the **Device Type** select **PinPad**.

5 In the **Device to Add** field select the appropriate PinPad device. Click **Add to Linked Devs**.

6 Repeat Steps 2-5 for all users, or menus or workstations or defaults that will use this PinPad device. Click **Exit** when you are finished.

7 Users must exit RecTrac and log back in for changes to take effect.

This concludes the MagTek IPAD Set up. Return to Set Up Your PlugNPay WebXPress Device above to continue with the WebXPress set up and configuration, if applicable.

Note: Once set up is complete, Vermont System recommends performing test transactions with the MagTek IPAD while in RecTrac debug mode.

Perform a test transaction and view the debug log. Search the log for "SwipeVal." The SwipeVal should display partial credit card numbers ONLY. If the SwipeVal displays complete credit card numbers, the MagTek IPAD is not configured properly. In this event, contact Vermont Systems Sales.

MagTek IPAD Installation Troubleshooting

MTIPADLIB.dll Not Found on Windows 7 Workstations

The MAGTEK_IPAD_DLL_REPLACE.exe is designed to find and replace all instances of the MTIPADLIB.dll on your Windows 7 workstation and make the required adjustments to your registry. In the event this fails, and the MTIPADLIB.dll cannot be found, you will receive errors when trying to log into RecTrac once the MagTek IPAD Pin pad device is created and linked in RecTrac. In this event, you can adjust the registry value manually.

1. Browse to C:\Program Files (x86)\MagTek\IPAD\MTIPADLIB\Library
2. Verify that the file MTIPADLIB.dll exists in this directory. If it does not, search your computer for the file MTIPADLIB.dll.

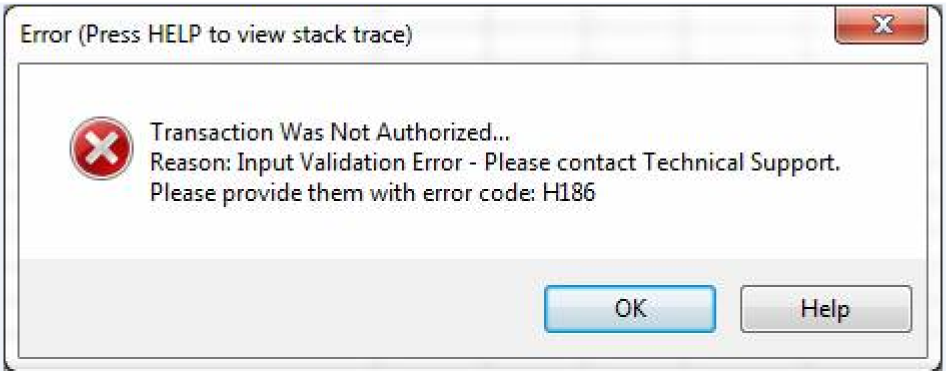
   When the computer finds the .dll, write down the location.
3. Go to Start • Computer.
4. Right-click on Computer and select **Properties.**
5. Select Advanced system settings
6. Select Environment Variables.
7. Under *System Variables,* highlight Path (you may have to scroll down).
8. Select **Edit**.
9. Go to the end of the variable value field and add the following. Do NOT include the quotation marks:

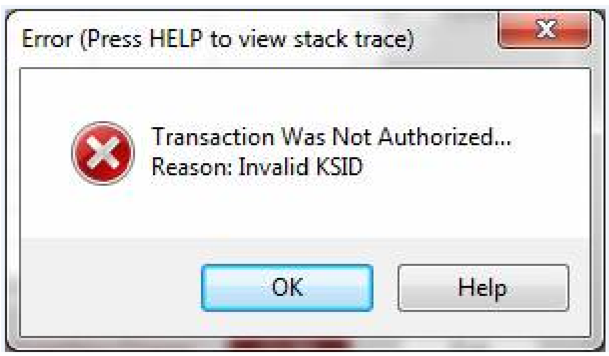
   ";C:\Program Files (x86)\MagTek\IPAD\MTIPADLIB\Library"
10. Click **OK**. Click **OK**. Click **OK**.
11. Restart/Reboot the workstation

Error Code H186 and Invalid KSID Errors

If you receive the following errors during processing, you have not registered the KSN with PlugNPay\WebXPress.

The KSN is unique to each MagTek IPAD. Contact Vermont Systems Sales in the event you receive these errors.





PAGE LEFT BLANK FOR DOUBLE-SIDED PRINTING