

REZSTREAM PROFESSIONAL CREDIT CARD PROCESSING MANUAL - MERCHANT PARTNERS

January 2011

TABLE OF CONTENTS

TABLE OF CONTENTS	2
ABOUT THIS MANUAL	4
CONTACT US	4
1. CONFIGURING THE CREDIT CARD GATEWAY	4
TRANSACTIONS.....	6
FRISK™ MANAGEMENT	8
Prevent Duplicate Transactions	7
Address Verification	8
Allow Credits	11
2. CONFIGURING REZSTREAM PROFESSIONAL	11
3. USER PASSWORDS AND PCI LOGGING OF ALL CREDIT CARD PROCESSING ACTIVITY	17
4. PROCESSING CREDIT CARD TRANSACTIONS	23
ADVANCE DEPOSITS	24
HOTEL PRE AUTH.....	28
New Card Presented at Check Out.....	36
RETAIL CHARGES	36
REFUNDS	39
5. PRINTING CREDIT CARD REPORTS	30
CREDIT CARD PROCESSING – BEST PRACTICES	33
CREDIT CARD SECURITY AND PCI COMPLIANCE INFORMATION	34
ACCESSING SENSITIVE CREDIT CARD DATA	35
CREDIT CARD STORAGE METHODS	36
CREDIT CARD PASSWORD ACCESS	36
PROPERLY TRAIN AND MONITOR ADMINISTRATIVE PERSONNEL	36
PCI COMPLAINT REMOTE ACCESS	36
PCI COMPLIANT WIRELESS NETWORKS	37
NETWORK SEGMENTATION (FIREWALL PROTECTION)	38
MAINTAIN AN INFORMATION SECURITY PROGRAM	38
REZSTREAM CONTACT INFORMATION	39

ABOUT THIS MANUAL

RezStream's optional credit card processing interface works with approved third party merchant account providers to provide unsurpassed convenience in credit card processing. Process credit card deposits, pre-authorize credit amounts (for the lowest rates), or process retail swiped transactions directly from within RezStream Professional property management software (PMS). Eliminate costly hardware, save time, money, and protect your valuable data.

This manual will walk you through configuring the credit card gateway and RezStream Professional PMS in order to begin processing credit card transactions. In addition, the manual provides step-by-step instructions for recording payments in RezStream Professional and printing reports to balance credit cards.

Topics included in this manual are:

1. Configuring the credit card gateway
2. Configuring RezStream Professional
3. User profiles, PCI logging, and deleting credit card data
4. Processing credit card transactions
5. Printing credit card reports
6. Payment cardholder information (PCI) standards

CONTACT US

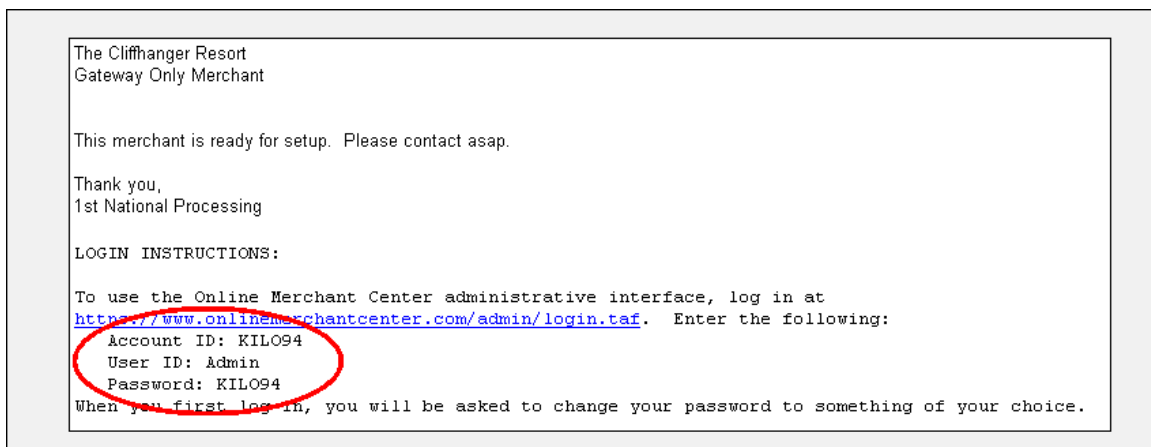
RezStream Help Desk: 303-872-0220

Email: support@rezstream.com

Support Hours: 8:00AM to 5:00PM, Monday through Friday, MST.

1. CONFIGURING THE CREDIT CARD GATEWAY

Once your property's Merchant Application and Agreement form is processed, you will receive an approval notification email that includes credit card gateway login instructions, an Account ID, User ID, and Password. A sample approval notification email is displayed below.



Click the link in the email (<http://www.onlinemerchantcenter.com/admin/login.taf>) to access the Online Merchant Center. Here, enter your Account ID, User ID, and Password under the Customer Login heading.

MerchantPartners
PaymentGateway

Your Payment Gateway
To E-Commerce
SUCCESS

Customer Login | Features | ACH Checks | Shopping Carts | Customer Support | Contact Us

Customer Login
Free Live Demo

Merchant Partners Tools

- ▶ Payment Gateway
- ▶ Virtual Terminal
- ▶ Credit Cards
- ▶ Recurring Billing
- ▶ Membership
- ▶ Wireless Devices

ACH Check Service

- ▶ ACH Checks
- ▶ Check Guarantee
- ▶ Check Conversion
- ▶ Card Present
- ▶ Debit Cards
- ▶ ACH Equipment

Shopping Carts

- ▶ Compatible Carts
- ▶ HTML Weblink
- ▶ Ebay Users
- ▶ Sample Code

Support

- ▶ Customer Support
- ▶ User Manuals
- ▶ FAQ's
- ▶ Certified Networks
- ▶ Fraud Prevention
- ▶ Visa CISP
- ▶ Resellers
- ▶ Contact Us

Welcome to Merchant Partners Support Central

We recognize the importance of a technical support department that is responsive to your needs. We understand that timely, correct answers to technical questions, setup questions, even simple "How do I..." questions are paramount to achieving maximum success with any business application. If you do not find the answers to your questions or issues, please email us and we will respond immediately.

Customer Login

Account ID
KIL094

User ID
Admin

Password

Login

Support Documentation

[Click Here To View The Documentation Download Page](#)

The support and training documentation files located in this website are all saved in Adobe Portable Document Format (PDF). You need the free Adobe Acrobat Reader to view and print the file. If you do not have the free reader, click on the icon below to download. Then follow the instructions to install.

Get Adobe Reader

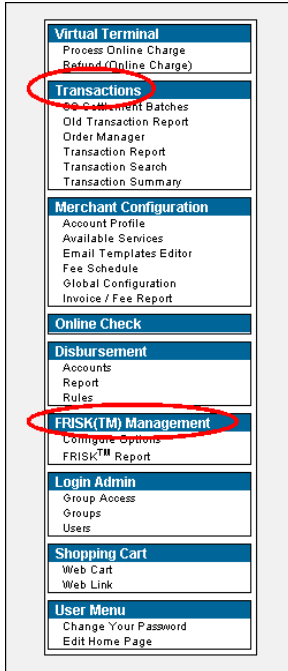
Click the Login button. Upon logging onto the Online Merchant Center for the first time, you will be prompted to change your password.



Be sure to save your Account ID, User ID, and Password. You will need this information each time you logon to the Online Merchant Center.

Once your password is changed, the Online Merchant Center home page is displayed. Use the links on the left-hand side of the page to update settings in the following sections:

- Transactions
- FRISK Management

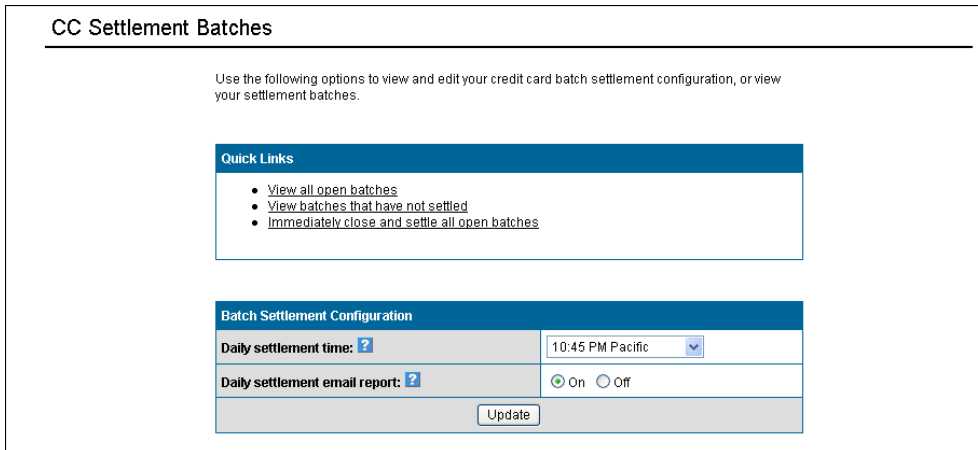


TRANSACTIONS

From the main navigation toolbar on the left of the Online Merchant Center page, click Transactions > CC Settlement Batches.



The CC Settlement Batches page is displayed. From this page you will use the fields in the Batch Settlement Configuration section to specify what time the credit card batch will be sent from RezStream Professional to the credit card gateway each night.



The drop-down “Daily settlement time” field is used for specifying the time the credit card batch will be sent each day. Set the “Daily settlement email report” radio button to “On” in order to receive a daily email detailing credit card transactions that were processed through the gateway.



Note that all times listed in the drop-down menu are in the Pacific time zone. Keep this in mind when selecting a daily settlement time. For example, if your property is in Rhode Island and you would like credit card transactions to be settled at 11:30PM nightly, you would select 8:30PM Pacific.

Batch Settlement Configuration	
Daily settlement time: ?	07:45 PM Pacific 08:00 PM Pacific 08:15 PM Pacific 08:30 PM Pacific 08:45 PM Pacific
Daily settlement email report: ?	<input checked="" type="radio"/> On <input type="radio"/> Off
<input type="button" value="Update"/>	



RezStream recommends setting your daily settlement time prior to midnight. With a setting prior to midnight, credit card transactions will be batched the same day they were processed.

FRISK™ MANAGEMENT

After configuring the Batch Settlement Configuration, click FRISK™ Management > Configure Options.

Virtual Terminal Process Online Charge Refund (Online Charge)
Transactions CC Settlement Batches Old Transaction Report Order Manager Transaction Report Transaction Search Transaction Summary
Merchant Configuration Account Profile Available Services Email Templates Editor Fee Schedule Global Configuration Invoice / Fee Report
Online Check
Disbursement Accounts Report Rules
FRISK(TM) Management <u>Configure Options</u> FRISK™ Report
Login Admin Group Access Groups Users
Shopping Cart Web Cart Web Link
User Menu Change Your Password Edit Home Page

PREVENT DUPLICATE TRANSACTIONS

In the General Controls section, click the Edit hyperlink that corresponds to the Prevent Duplicate Transactions heading. This feature tracks recently processed transactions to ensure that the same transaction amount for the same card is not authorized more than once in a given time period.

By reducing the time interval, you can still receive duplicate transactions if applicable.

General Controls		
Option	Status	
IP Blocking	Inactive	Edit
Cramming Protection	Inactive	Edit
Brute Force Attack Protection	Active	Edit
IP Activity Limit	Inactive	Edit
Large Transaction Notification	Inactive	Edit
Prevent Duplicate Transactions	Active	Edit
Ship Only to Billing Address	Inactive	Edit
Validate Email Domain	Inactive	
Domain Blocking	Inactive	Edit
Reject Free Email Addresses	Inactive	Edit
Country Blocking	Inactive	Edit
Restrict Transaction Source	Inactive	Edit




Set the Status to Active and the Duplicate check duration to 1 minute.

Duplicate Transaction Checking	
Status:	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
Include Merchant Order Number in Dup Check:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Include Consumer Name in Dup Check:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Duplicate check duration:	1 <input type="text"/> minutes
Ship Only To Billing Address	
Status:	<input type="radio"/> Active <input checked="" type="radio"/> Inactive
Validate Email Domain	
Status:	<input type="radio"/> Active <input checked="" type="radio"/> Inactive
Update	

Click the Update button to save the changes.

ADDRESS VERIFICATION

Next, click the Edit hyperlink that corresponds to the Address Verification heading. Address verification matches the known address information associated with the given credit card number against the billing address information provided by the user. If the information does not match, the transaction is declined.

Online Charge Controls		
Option	Status	
Address Verification 	Visa: <i>Active</i> Master Card: <i>Active</i> Discover Card: <i>Inactive</i> Amex Card: <i>Active</i> Diner's Club: <i>Inactive</i> JCB: <i>Inactive</i>	Edit
Require CVW2 	Visa: <i>Not Required</i> Master Card: <i>Not Required</i> Amex: <i>Not Required</i> Discover: <i>Not Required</i>	Edit
Negative Account Blocking CC 	Active: Base Level	Edit

In the Address Verification Status table, click the Active button for each credit card type accepted at your property.

Address Verification Status	
Visa	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
Master Card	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
American Express	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
Discover Card	<input type="radio"/> Active <input checked="" type="radio"/> Inactive
Diner's Club	<input type="radio"/> Active <input checked="" type="radio"/> Inactive
JCB	<input type="radio"/> Active <input checked="" type="radio"/> Inactive

In addition, set the level of match required for an approved transaction. RezStream suggests setting the level of match to "Either Address or Postal Code must match." In order to provide a high level of customer service security to guests, RezStream suggests setting the last two fields on the Address Verification Options page to "Accept these cards." With this setting, cards issued outside of the United States that are not setup to handle AVS, will not be automatically declined. In addition, if the AVS system for a guest's card is temporarily down, the card will not be automatically declined.

Address Verification Options

Verification Requirements

IMPORTANT NOTICE:
Please read BEFORE proceeding with AVS option configuration!

Transactions which are declined due to non-match of AVS information are still authorized by the credit card network, but the sale amount will NOT be charged to the credit card holder's account and *will not* be deposited to your bank account.

Click [here](#) for full details.

No Match Required
 Only Address must match
 Only Postal Code Must Match
 Either Address or Postal Code must match
 Either Address or 9 Digit Postal Code must match
 Address and 5 digit Postal Code must match
 Address and 9 digit Postal Code must match

AVS can not be performed on all cards, for example some cards issued outside of the U.S. Please select how you would like such cards to be handled.

Accept these cards
 Reject these cards

Sometimes, even though AVS can be performed on a certain credit card, the AVS system for the consumer's bank may be temporarily unavailable. Please select how you would like such cards to be handled.

Accept these cards
 Reject these cards



WARNING – SETTING AVS TO “NO MATCH REQUIRED” WILL INCREASE YOUR PROPERTY’S CREDIT CARD PROCESSING RATES!

ALLOW CREDITS

The last setting that needs to be configured is the option for allowing credits. By default, submitting standalone credits/refunds is disabled. Use the following steps to enable this feature.

1. At the bottom of the FRISK™ Management > Configure Options page, click the Edit button to the right of the Allow credits heading.

API Controls		
Option	Status	
Allow credits	Active	Edit
Merchant PIN	Inactive	Edit
Account Number 3DES Encryption	Inactive	Edit

2. The IP Credit Security page is displayed. In order to reduce the risk of fraud, Internet IP addresses of the computer(s) used for refunds must be registered. In most network scenarios, only the IP address for the router must be registered.

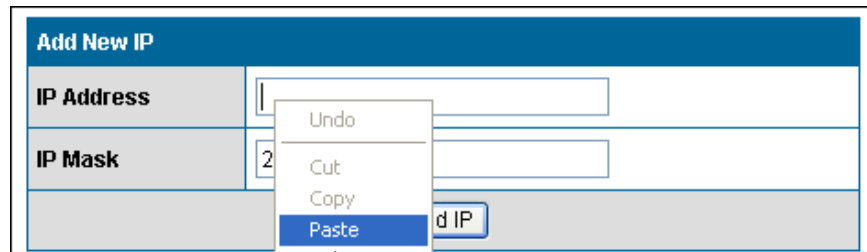
- a. In order to locate your computer's IP address, be sure you are connected to the Internet and then open a web browser, for example, Internet Explorer.
- b. Enter the following URL: <http://www.whatismyip.com>.
- c. Your computer's IP address is automatically displayed at the top of the web page.



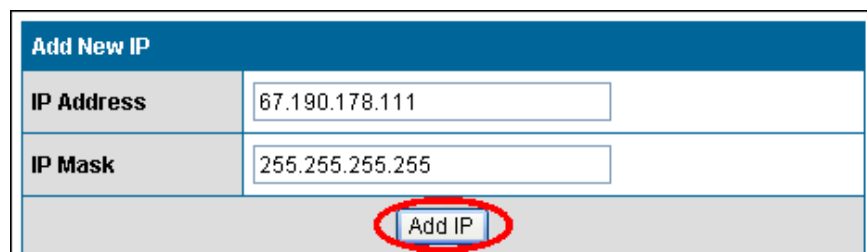
- d. Click the Copy Your IP link.



- e. Click inside the IP Address field, right-click, and paste your IP address.



- f. Click the Add IP button.



Follow steps 2a – 2f above at each workstation that will process credits. Multiple workstations must only be configured if your property does NOT utilize a router for Internet access.

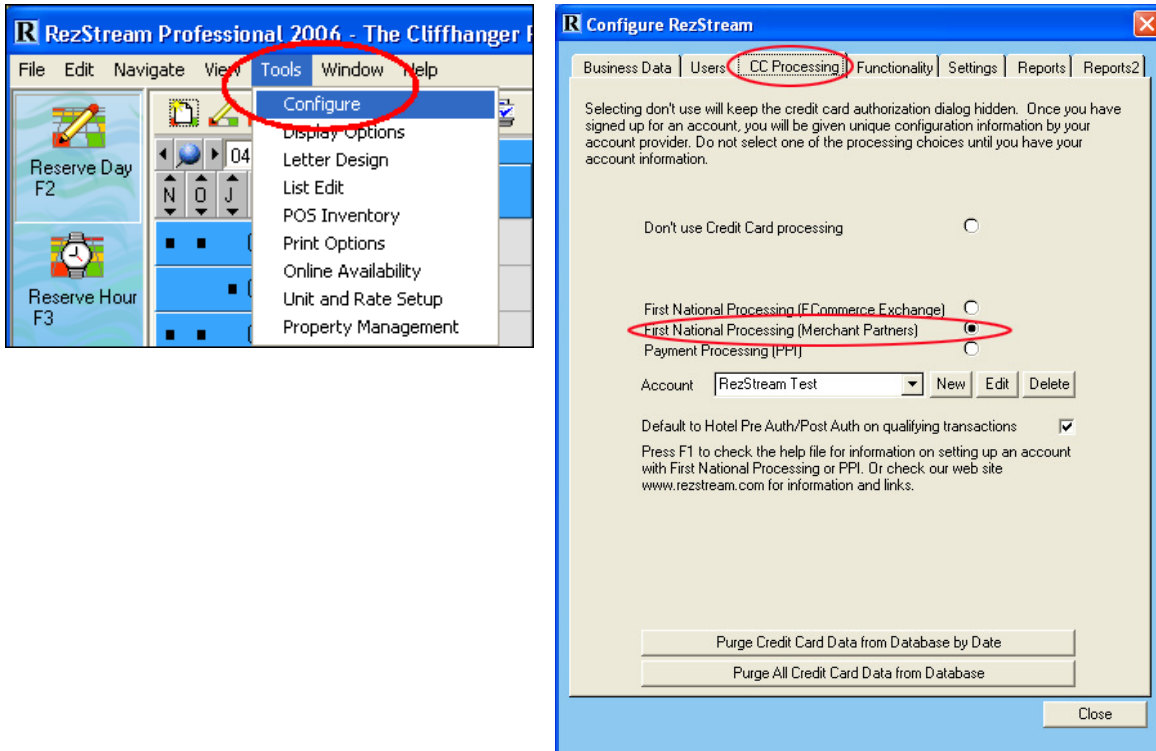


Properties that use RezStream Professional in multiple locations will need to add the IP address for each workstation that is processing transactions at each property.

2. CONFIGURING REZSTREAM PROFESSIONAL

After completing the steps listed in section 1. **Configuring the Credit Card Gateway**, you are ready to configure RezStream Professional to accept credit card transactions. Use the following steps to configure RezStream Professional.

1. Access the credit card processing configuration fields in RezStream Professional by clicking Tools > Configure and selecting the CC Processing tab.
2. In the CC Processing tab, select the radio button for First National Processing (Merchant Partners).



3. Click the New button to configure your account.

4. In the Description field, enter the name of your property.

Edit Gateway Account

Enter a description for the account and the UserID and Sub Account if used

Description:

User ID:

Sub Account:

Save Close

5. In the User ID field, enter the Account ID number given to your property in the approval notification email.

The Cliffhanger Resort
Gateway Only Merchant

This merchant is ready for setup. Please contact asap.

Thank you,
1st National Processing

LOGIN INSTRUCTIONS:

To use the Online Merchant Center administrative interface, log in at <http://www.onlinemerchantcenter.com/admin/login.taf>. Enter the following:

Account ID: KIL094
User ID: Admin
Password: KIL094

When you first log in, you will be asked to change your password to something of your choice.

Either copy and paste the Account ID from the approval notification email to the Edit Gateway Account window or manually enter it exactly as it is listed in the email.

Edit Gateway Account

Enter a description for the account and the UserID and Sub Account if used

Description:

User ID:

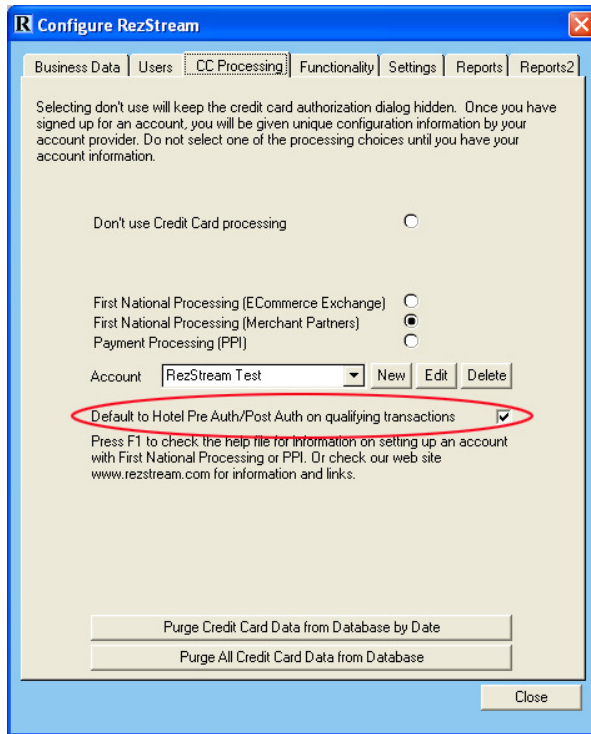
Sub Account:

Save Close

Copy the User ID from the approval notification email.

6. The Sub Account is not required and can be left blank. Click the Save button.

7. In order to receive the best possible credit card processing rates, check the Default to Hotel Pre Auth/Post Auth on qualifying transactions field.



RezStream strongly recommends structuring your payment schedule so that guest credit cards are only pre-authorized at check in, with actual payments posted upon check out. This scenario, utilizing a Lodging credit card account rate, ensures the lowest possible credit card processing fees.



If the majority of full payments are taken at your property either in advance of the guest's arrival date or at check in, RezStream recommends using a Retail, NOT Lodging, credit card account. (See page 27 of this manual for the difference between Lodging accounts and Retail accounts.)

3. USER PASSWORDS AND PCI LOGGING OF ALL CREDIT CARD PROCESSING ACTIVITY

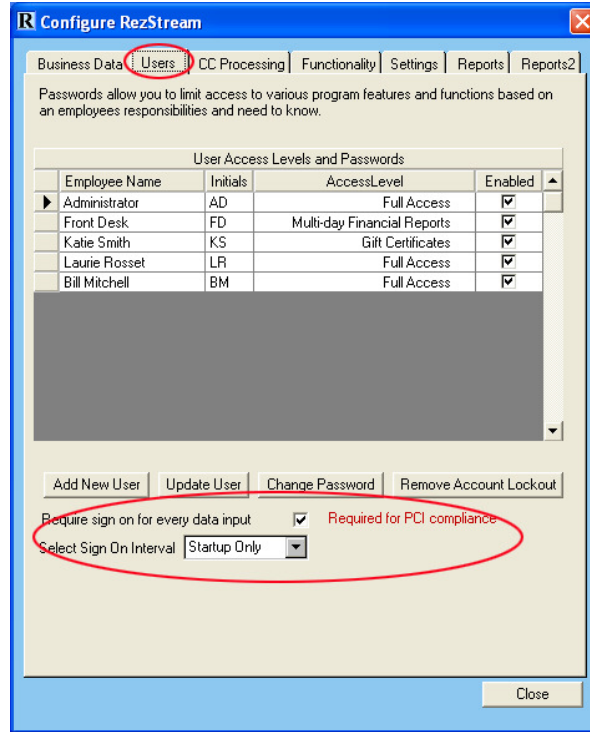
New rules went into effect on July 1, 2010 that requires all credit card processing applications to be PCI (Payment Cardholder Information) compliant. Because of these new required standards, RezStream now requires its customers to utilize "Strong passwords" (7-10 characters, with one upper case, and one special character) to enter, and navigate, within RezStream Professional 2008.0 and newer. In addition, RezStream Professional users are also required to have unique user names and passwords. Due to PCI compliance, these passwords must be used every time a user creates, modifies, or edits any reservation or payment.

Another integral requirement of PCI compliance is the security of all credit card data, ability to delete credit card numbers, and the logging of all such user behavior. This section will cover how to create user names, make sure your PCI transaction logging is activated, and how to delete sensitive credit card information.

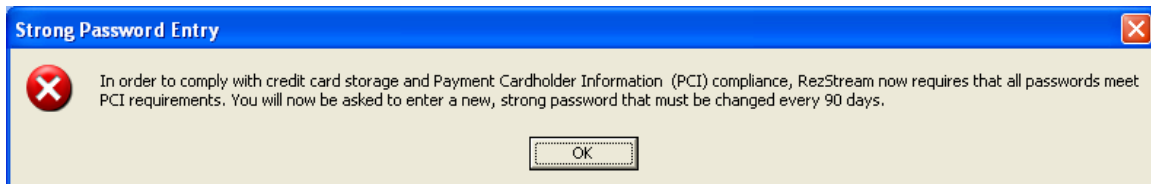
Creating User Profiles:

All user profiles are created by the manager or owner of each property.

1. From the top toolbar in RezStream Professional, go to Tools > Configure > Users.



2. Click on the Add New User tab. All new users will have a default password of "pass." When each new user enters RezStream for the first time they will be asked to change their password. (See diagrams below.)
3. Under no circumstances should your employees "pool or share" a user profile or password. Each employee is required by PCI standards to have their own unique user name and password.



Enter New Password

Bill Mitchell

Your password has expired. Enter your old password and a new password. Your new password must be between 7 and 10 characters. It must contain at least one capital letter, one lower case letter, and one numeric character. Spaces are not allowed. You will be prompted to change your password every 90 days.

Old Password: [masked]

Enter new password twice

New Password: [masked]

New Password: [masked]

Ok

PCI Logging of All Credit Card Activity:

PCI standards require that software application log all credit card processing activities. RezStream tracks all times, details, and user information for every data entry within RezStream Professional. Detailed reports are available within the **Reports Screen > Miscellaneous > Log of Activity area**.



WARNING! You should **NEVER** uncheck the “Require sign on for every data input” within **Tools > Configure > Users**. This will disable PCI compliance requirements.

Configure RezStream

Business Data | **Users** | CC Processing | Functionality | Settings | Reports | Reports2

Passwords allow you to limit access to various program features and functions based on an employees responsibilities and need to know.

User Access Levels and Passwords

Employee Name	Initials	AccessLevel	Enabled
Administrator	AD	Full Access	<input checked="" type="checkbox"/>
Front Desk	FD	Multi-day Financial Reports	<input checked="" type="checkbox"/>
Katie Smith	KS	Gift Certificates	<input checked="" type="checkbox"/>
Laurie Rosset	LR	Full Access	<input checked="" type="checkbox"/>
Bill Mitchell	BM	Full Access	<input checked="" type="checkbox"/>

Add New User | Update User | Change Password | Remove Account Lockout

Require sign on for every data input Required for PCI compliance

Select Sign On Interval: Startup Only

Close

Purging Credit Card Data:

PCI requirements also stipulate that any application that processes credit cards have the ability to purge allowable (encrypted card numbers only) credit card data. RezStream Professional version 2010.8 and newer has multiple ways to purge allowable credit card data.

1. To delete individual card numbers, card numbers associated with invoices, and all card numbers for a customer contact, navigate to the Contact Data Screen>Details Tab (Right side of the screen)
2. Double left click in the area where credit cards are entered to pick which card you would like to purge.
3. Click on the X icon to the right of the credit field and enter your PCI required strong password.
4. Choose the option you wish to delete.
 - a. Selected card data
 - b. Invoice card data
 - c. Contact card data.

Contact Data Screen Credit Card Details Tab:

The screenshot displays the RezStream Professional 2010 interface for a contact named 'Lodge at Rock Creek (Test)'. The 'Contact Invoice History' tab is active, showing a table of invoices with columns for Inv #, Entered, Begins, Ends, Start Unit, Length, and Total. A red arrow points to the 'X' icon next to the 'Credit Card Data' field in the 'Payment Data' section of the 'Details' tab.

Inv #	Entered	Begins	Ends	Start Unit	Length	Total
1659	5/5/2009	5/6/2009	5/12/2009	302 KS	7	\$87
1308	12/17/2008	9/9/2008	9/12/2008	401 KS	4	\$2.46
563	11/10/2005	11/10/2005	11/12/2005	402 QS	3	\$64
475	8/12/2005	8/14/2005	8/20/2005	306 DD	7	\$1.43
471	8/10/2005	8/10/2005	8/13/2005	203 KS	4	\$83
464	8/8/2005				3	\$1
460	7/19/2005	7/19/2005	7/21/2005	204 D	3	\$59

Contact Invoice History 7/28

Starts: **Fri September 8, 2002** Departs: **Mon Sept 18** Length: **2**

Adult 2 6-10 2 Packages

Child 0 1-5 0

Checked In: x

Checked Out: x

Payment Data

Confirmation # 1659 AD C

Payment Data: Visa Adult 2 Child 1

Swipe Card... 6-10 1-5

Credit Card Data: Arrive Depart

Exp 2009 Letter Standard

Checked In Out

Batch Print Flag

Vehicle Description

Global Credit Card Purge Options:

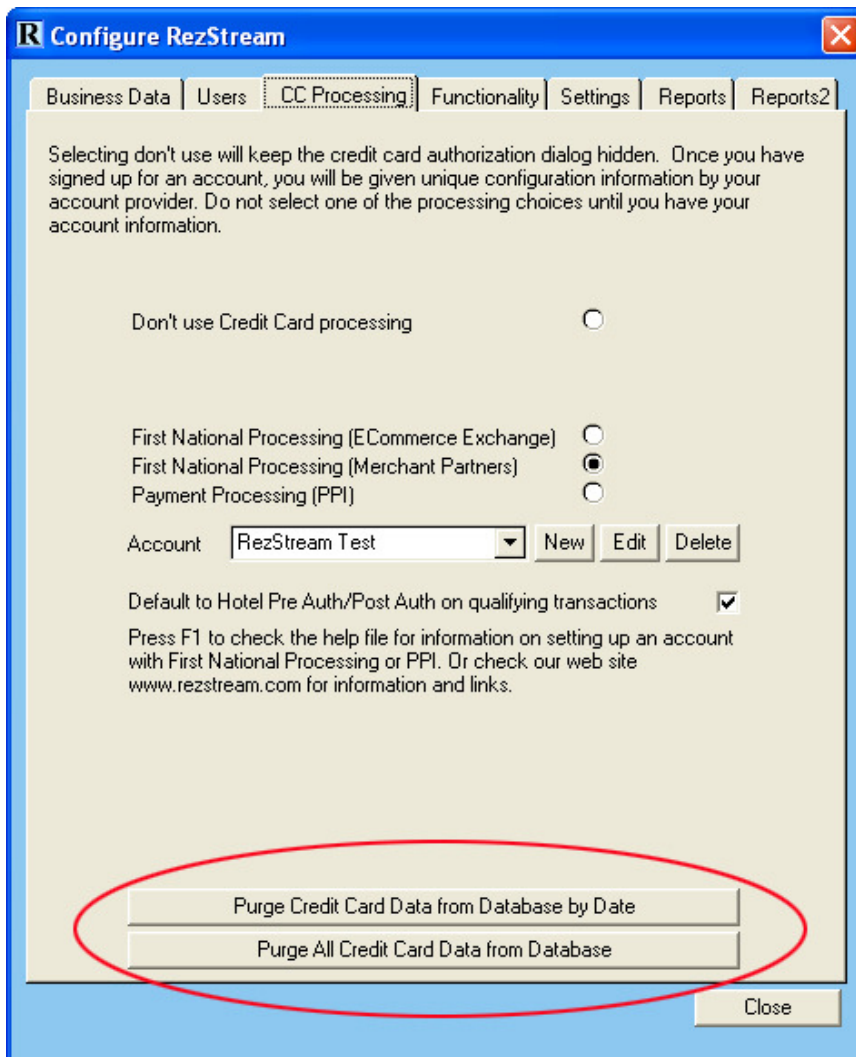
PCI compliance regulations also require that programs that process and store allowable credit card data (encrypted card numbers only) be purged when the cards are no longer needed for any existing advance reservation. RezStream STRONGLY recommends that all credit card numbers be purged within one year (or less) of entry into the program.

The following steps explain how to globally purge credit card data.

1. From the top toolbar in RezStream Professional, go to Tools > Configure > CC Processing.
2. Choose between one of two options for purging all card data.
 - a. Purge data by date range. The system automatically defaults to one year ago.
 - b. Purge ALL credit cards within the system.



Only administrators with a level 10 user clearance will be able to view and use these global credit card data options.



4. PROCESSING CREDIT CARD TRANSACTIONS

There are several types of credit card transactions that can be processed through RezStream Professional, including:

- Advance Deposits
- Hotel Pre-Authorization
- Retail
- Refunds

Steps for processing each type of credit card transaction are detailed in this section.

ADVANCE DEPOSITS

This section describes the process of recording advance deposits in RezStream Professional. Please note that credit card transactions processed prior to check-in are charged at a higher credit card processing rate. If possible, RezStream recommends altering your property's deposit rules to allow you to follow the Hotel Pre Auth steps described in the following section. If your property is unable to alter its deposit rules, RezStream recommends obtaining a **Retail** credit card processing account. With a Retail account, credit card processing rates will be higher than when using the Hotel Pre Auth rate described in the following section, but lower than the advance deposit rate. For additional information, please contact RezStream sales at 866-360-8210.

After making a reservation, the guest's personal information is displayed on the Contact Data screen. Click the Record Transaction button to take an advance deposit.

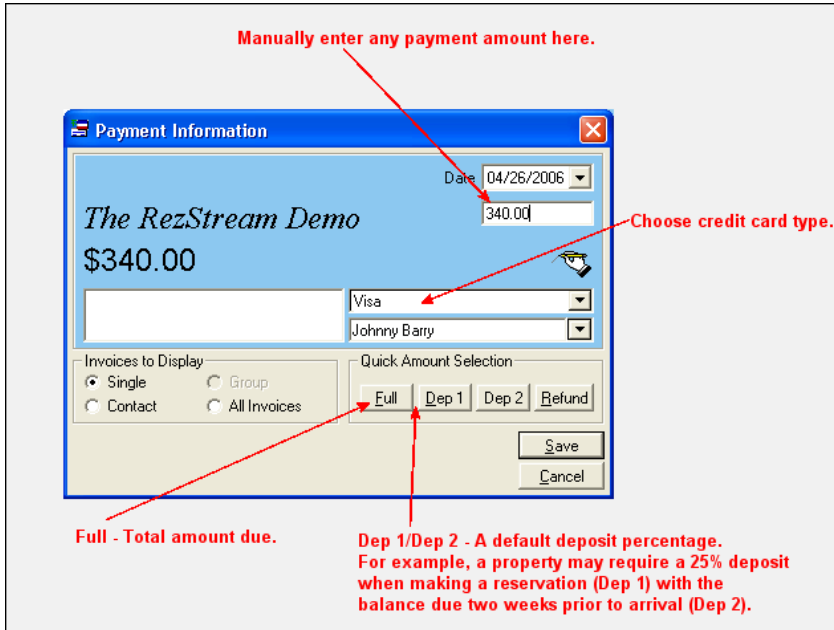


An alternative method for taking an advance deposit is to click the Add button in the Payments tab at the bottom of the screen.

The screenshot displays the 'Contact Invoice History 9/22' window. The top toolbar contains a 'Record Transaction' button, highlighted with a red arrow. The main area shows a table of invoice history with columns: Inv #, Entered, Begins, Ends, Start Unit, Length, Total, Paid, and Confirmation. Below the table, reservation details are shown for a stay from Tue, May 02, 2006 to Sat, May 06, 2006. The 'Payments' tab is active, showing a 'First Deposit' and 'Second Deposit' section. The 'Add...' button at the bottom of the Payments section is circled in red.

Inv #	Entered	Begins	Ends	Start Unit	Length	Total	Paid	Confirmation
525	4/26/2006	5/2/2006	5/5/2006	105	4	\$754.14	\$0.00	525
491	4/3/2006	4/2/2006	4/4/2006	101	3	\$498.05	\$0.00	491
417	2/8/2006	2/7/2006	2/12/2006	103	6	\$731.94	\$280.00	417
384	1/25/2006	2/1/2006	2/1/2006	101	1	\$110.90	\$0.00	384
321	1/17/2006	1/21/2006	1/24/2006	102	4	\$443.62	\$0.00	321
290	1/11/2006	1/8/2006	1/7/2006	BIKE2	0	\$33.27	\$0.00	290
273	1/11/2006	1/10/2006	1/9/2006	BOAT1	0	\$221.80	\$221.80	273
236	1/11/2006	1/11/2006	1/10/2006	BALL1	0	\$1,109.00	\$500.00	236
56	11/3/2005	11/8/2005	11/11/2005	112	4	\$443.62	\$200.00	56

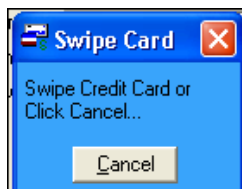
The Payment Information window is displayed. First, use the drop-down field to specify the credit card type. Then, either enter a payment amount in the payment amount field or select one of the Quick Amount Selection buttons to choose Full (the total amount due) or Dep 1/Dep 2 (a default deposit percentage).



After specifying a dollar amount or clicking one of the Quick Amount Selection buttons, click Save.

The Online Credit Card Processing window is displayed along with a popup window prompting you to swipe a credit card or click Cancel. In the case of advance deposits, the guest is not normally in front of you with a credit card to swipe. Use the following steps to record an advance deposit.

1. Click the Cancel button.



2. Enter the card number and four-digit expiration date (mmyy).



The red square to the right of the credit card number indicates that the card was NOT swiped.

3. Click the Process Transaction button. Upon completing the transaction, a Transaction Successful window is displayed. Click OK.

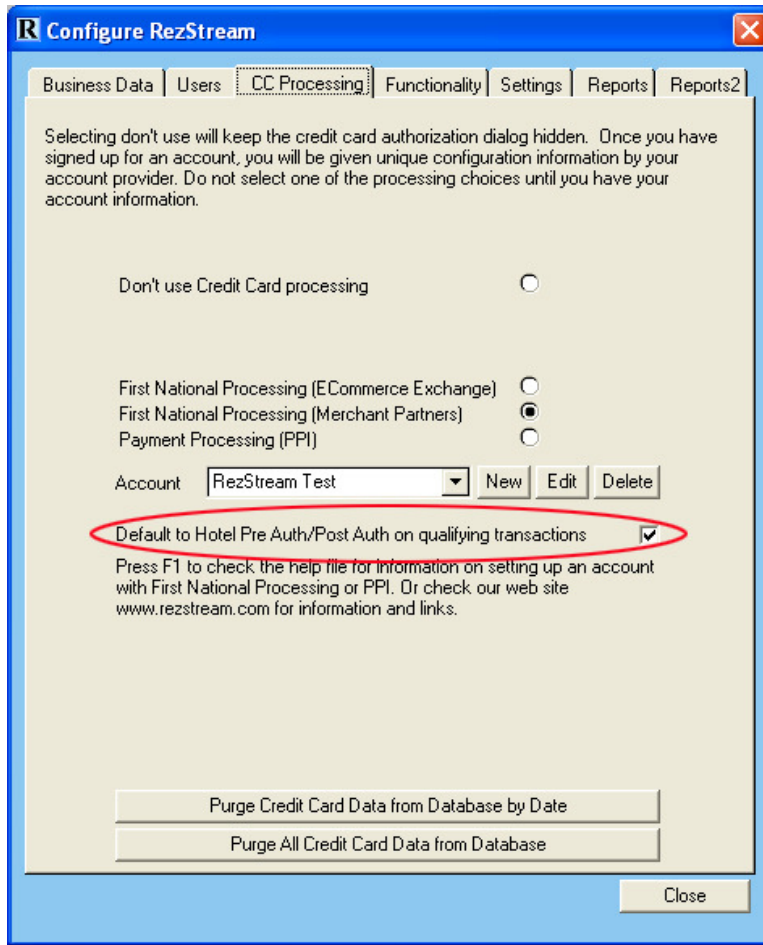
HOTEL PRE AUTH

The Hotel Pre Auth method of authorizing a credit card at check in and then posting the charge at check out is the recommended way to process credit card transactions for the lowest possible rate.

With this method, the guest's credit card is swiped at check in and the card is authorized for a specific dollar amount. This "holds" the stated credit amount and makes it available for actual approval at check out time. However, this charge is not actually posted to the guest's credit card until check out.

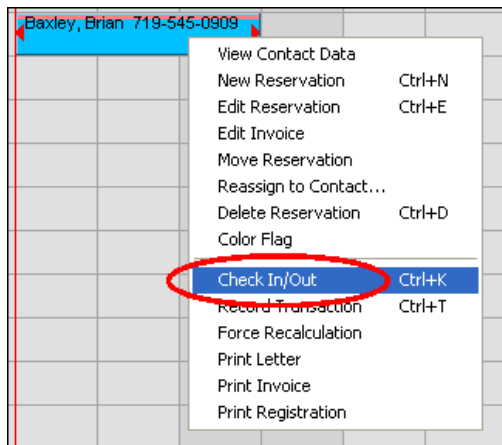


Earlier in Section 2. Configuring RezStream Professional, the system was configured to "Default to Hotel Pre Auth/Post Auth on qualifying transactions."

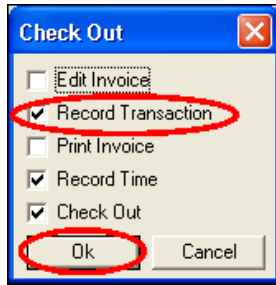


Use the following steps for processing a Hotel Pre Auth transaction.

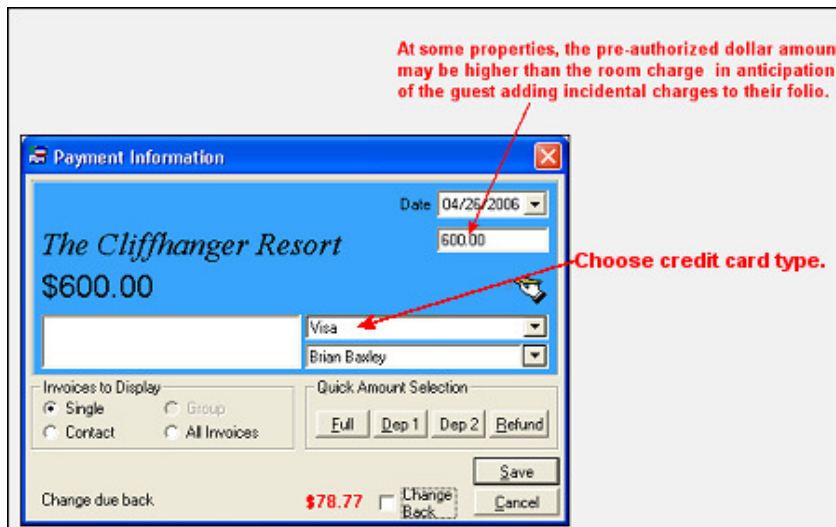
1. From the Daily screen, right-click a reservation and select Check In/Out.



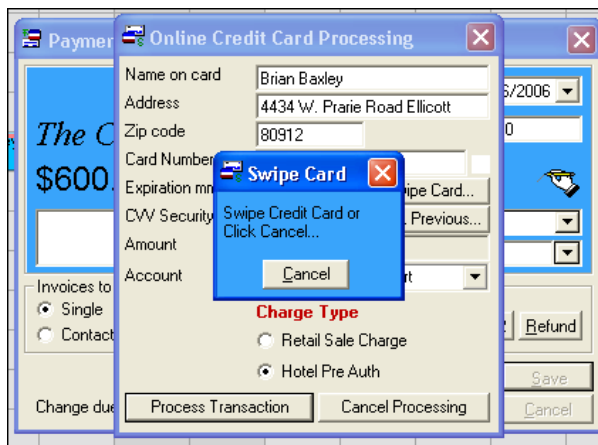
2. Enter a checkmark in the Record Transaction checkbox and click OK.



3. The Payment Information window is displayed. Here, use the Quick Amount Selection buttons or enter a dollar amount in the payment amount field. Whatever amount is specified in the payment amount field is the amount authorized on the guest's credit card. Many times, this amount may include not only room charges but also a percentage in addition to room charges in anticipation of incidental charges.



4. After clicking the Save button in the Payment Information window, swipe the guest's credit card.



- The box next to the card number turns green indicating that you have swiped the card. In addition, because the transaction is being processed on the guest's arrival date, the Hotel Pre Auth Charge Type is available. Hotel Pre Auth is the default RezStream Professional Charge Type and should not be changed.

- Click the Process Transaction button. Once the charge is successfully processed, a message similar to the one below is displayed. Click OK to complete the Pre Auth.

- The authorized charge is posted to the guest's credit card at check out. To check the guest out, right-click the reservation on the Daily screen and select Check In/Out. In the Check Out window, be sure the option for Record Transaction is selected and click the OK button.

8. The Payment Amount window is displayed. Click the Full button to display the total balance due. With the Visa credit card type chosen, click the Save button.

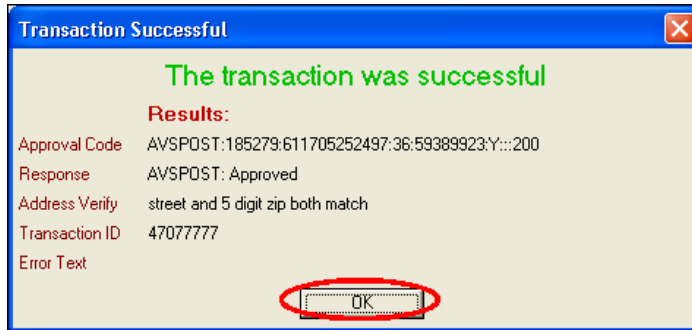
9. The Swipe Card window is displayed. Because the card was swiped at check in, click the Cancel button.



If the guest's credit card is swiped at check in, it does not need to be swiped again at check out.

10. The option for Post Hotel Pre Auth Charges is selected by default in RezStream Professional. Click the Process Transaction button to post the guest charges.

11. The charge is posted to the guest's credit card and a message is displayed indicating that the transaction was successfully processed. Click OK to complete the transaction.



NEW CARD PRESENTED AT CHECK OUT

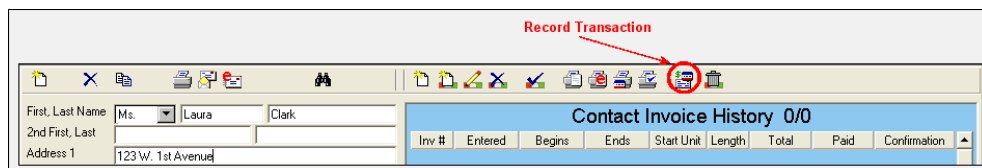
From time to time, a guest may ask to check out with a card that was NOT presented at check in. In this scenario, a payment can be recorded for the amount due using a Charge Type of "Retail Sale Charge."

In this scenario, the credit card processing rate will be slightly higher than a Hotel Pre Auth charge. Due to the higher rate, RezStream recommends asking the guest at check in to provide the card they plan to use for final payment at check out.

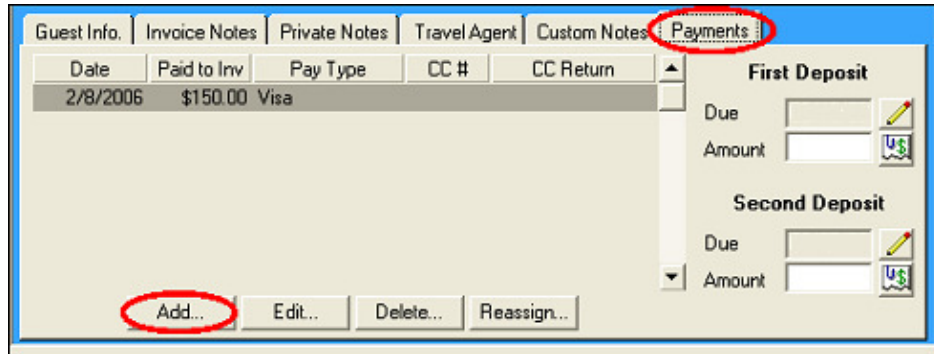
RETAIL CHARGES

Retail charges, including full payment at check in, boat rentals, gift shop sales, horseback rides, and jeep tours (just to name a few), can be processed through the credit card interface. Use the following steps to process a retail charge.

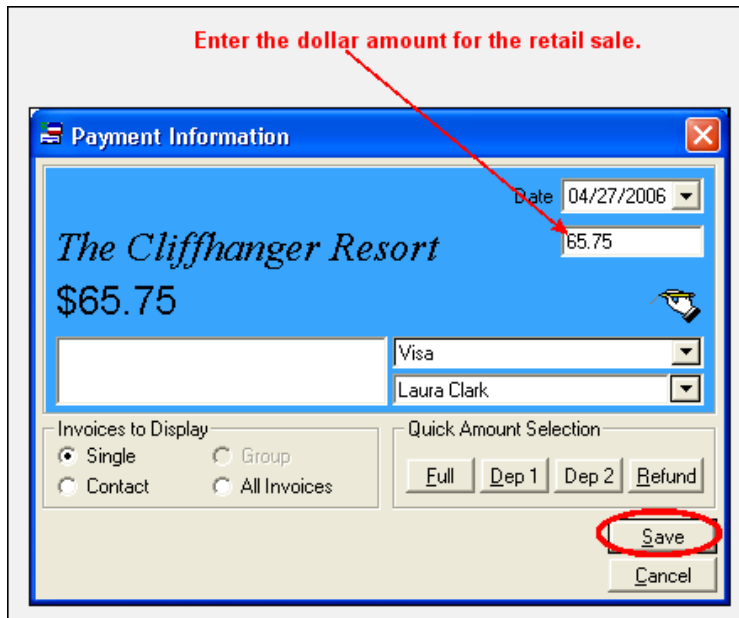
1. From the Contact Data screen, choose either:
 - A. The Record Transaction button.



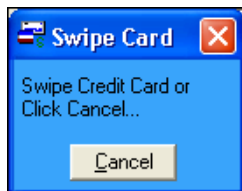
B. The Add button on the Payments tab.



2. The Payment Information window is displayed. In the payment amount field, enter the dollar amount for the retail sale and click the Save button.



3. The Swipe Card window is displayed. For the lowest possible credit card processing rate, swipe the credit card being used for the retail sale. If the card is not available for swiping, press the Cancel button and enter the card manually in step #4.



- The Online Credit Card Processing window is displayed. Set the Charge Type to Retail Sale Charge and click Process Transaction.

Online Credit Card Processing

Name on card: Laura Clark
 Address: 123 W. 1st Ave. Aspen
 Zip code: 81650
 Card Number: 4377540013160289
 Expiration mmyy: 0608
 CVV Security code:
 Amount: 65.75
 Account: The Cliffhanger Resort

Charge Type
 Retail Sale Charge
 Hotel Pre Auth

Process Transaction Cancel Processing

Green box indicates the card was swiped.

- The Transaction Successful message is displayed. Click OK to complete the Retail charge.

Transaction Successful

The transaction was successful

Results:

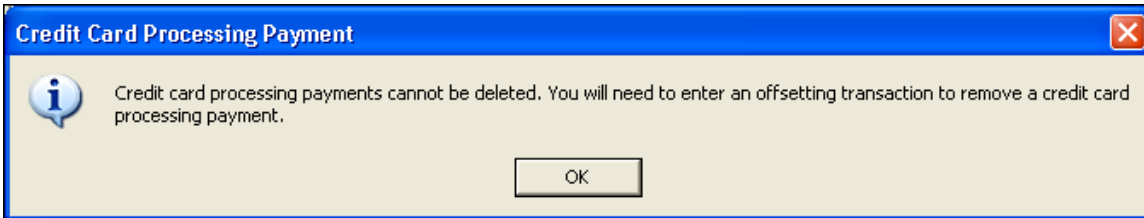
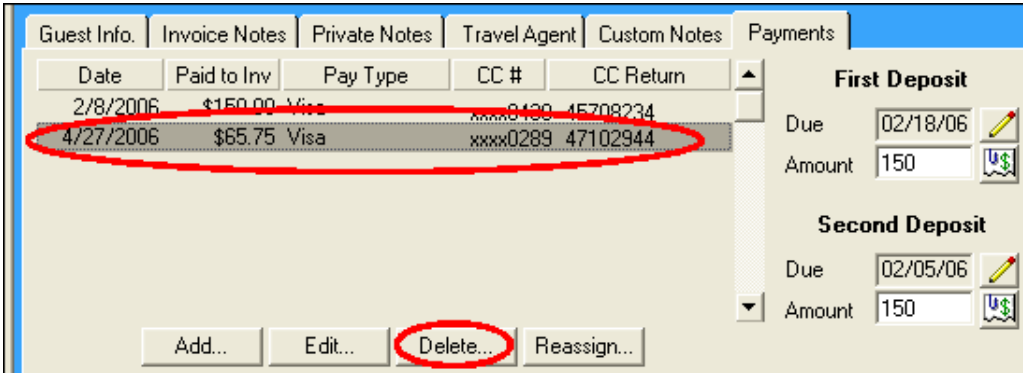
Approval Code: AVSSALE:018844:611802000654:36:59390303:Y:::165
 Response: AVSSALE: Approved
 Address Verify: street and 5 digit zip both match
 Transaction ID: 47102944
 Error Text:

OK

REFUNDS

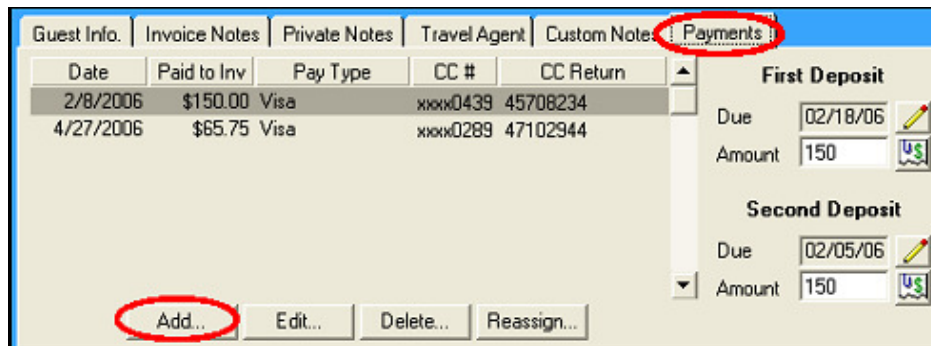
RezStream Professional added the ability to do “independent refunds” (refunds that do not require a previous transaction reference) in version 2008.3.0. This new feature allows full refunds, partial refunds, and the ability to refund payments originally processed through the RezStream Booking Engine. Simply type a minus symbol before the amount you wish to refund in the payment dialogue screen and select the card you wish to refund to in the actual payment window.

RezStream customers using a version older than 2008.3.0 must follow the instructions below for processing refunds. Payments processed through the credit card interface cannot be deleted from the Contact Data screen. If a credit card transaction is highlighted in the Payments tab and the Delete button is pressed, the following message is displayed.



Use the following steps to refund a payment processed through the credit card interface.

1. From the Payments tab on the Contact Data screen, click Add.



- In the payment amount field, enter the refunded amount and click the Save button.

Payment Information

Date: 04/27/2006

The Cliffhanger Resort
(\$65.75)

Payment Amount: -65.75

Card Type: Visa
Name: Laura Clark

Invoices to Display:
 Single
 Group
 Contact
 All Invoices

Quick Amount Selection:



Be sure to either select the “Refund” button to process a full refund or use a minus symbol before any dollar amount that is manually entered.

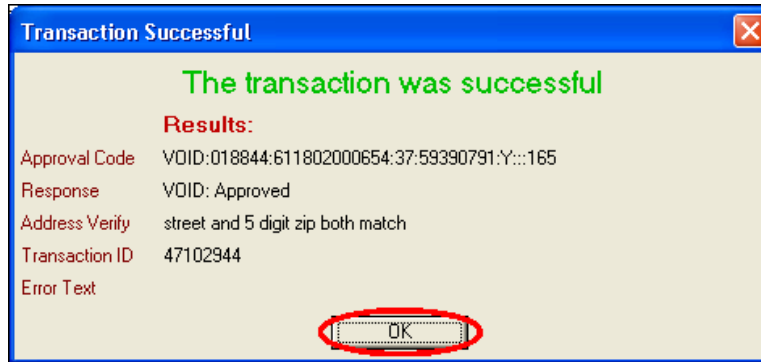
- The Choose Transaction to Credit window is displayed. Highlight the transaction that is being refunded and press the Process Credit button.

Choose Transaction to Credit

You must pick the transaction that you wish to credit. The amount that you are crediting cannot be greater than the transaction picked. You cannot credit a card that has not been previously charged.

Payment Date	Card Number	Amount	Transaction ID
04/27/2006	xxxx0289	65.75	AVSSALE:018844:611802000654:36:59390303:Y:::165:47102:
03/11/2006	xxxx0439	-5.00	VOID:009359:607013250190:29:57572527:Y:::500:45708234
03/11/2006	xxxx0439	5.00	AVSSALE:009359:607013250190:29:57572515:Y:::500:45708:

- A message is displayed indicating that the refund was successfully processed. Click OK to complete the refund.



5. PRINTING CREDIT CARD REPORTS

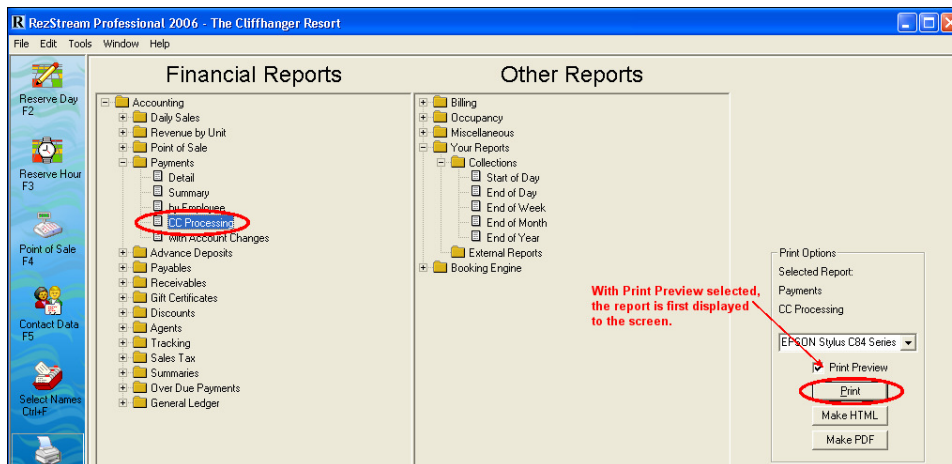
Credit card processing reports can be printed from both RezStream Professional and the Online Merchant Center. In order to be sure there are no discrepancies between the two systems, RezStream recommends printing daily activity reports from both systems and balancing the two prior to sending the credit card batch from the Gateway each night.

Use the following steps to balance the two systems.

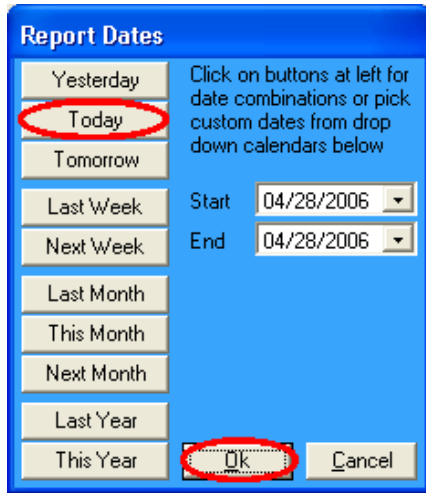
- From RezStream Professional, click the Reports F7 button on the main left-hand toolbar.



- In the Payments folder, highlight the CC Processing report and click the Print button. With the Print Preview checkbox selected, the report is first displayed to the screen.



- Click Today in the Report Dates dialog window. The Start and End dates default to the current date. Click the OK button.



- The report is displayed to the screen. The “Invoice #/Auth Code” field will display the actual approval number for each successful credit card transaction. If necessary, you may compare this number to open batches, or settled batches, displayed in the Online Merchant Center.

Payments Received								for: 04/28/2006 - 04/28/2006
Date	Employee	Payee	Trans ID	Invoice # / Auth Code	Card #	Acct #	Amount	
MPM9X								
Visa								
4/28/2006	AD	Mark Kleinsmith	47121592	AVSSALE:034858.611821503	xxxx0439	MPM9X	\$3.40	
				828:39.59420567:Y::340				
4/28/2006	AD	Mark Kleinsmith	47121592	VOID:034858.611821503828:	xxxx0439	MPM9X	(\$3.40)	
				38:59424435:Y::340				
4/28/2006	AD	Fisher DeBerry	47124397	AVSSALE:090237.611822504	xxxx0439	MPM9X	\$125.33	
				921:39.59424465:Y::12533				
4/28/2006	AD	Carmello Anthony	47124406	AVSSALE:017324.611822502	xxxx0439	MPM9X	\$99.09	
				366:39.59424474:Y::9909				
4/28/2006	AD	Sonny Lubick	47124417	AVSSALE:023852.611822006	xxxx0439	MPM9X	\$75.87	
				236:39.59424485:Y::7587				
							\$ 300.29	
							MPM9X \$ 300.29	
Total							\$ 300.29	

- Logon to the Online Merchant Center (<http://www.onlinemerchantcenter.com>).
- Click Transactions > Order Manager.



- In the Report Options table, select the radio buttons for Show All Orders and Show Today's Orders and click the View button.

Use the following options to generate a list of orders

Report Options	
Order Types	<input checked="" type="radio"/> Show All Orders <input type="radio"/> Show Only Open Orders <input type="radio"/> Show Only Completed Orders
Date Range	<input type="radio"/> Show All Orders <input checked="" type="radio"/> Show Today's Orders <input type="radio"/> Show Yesterday's Orders <input type="radio"/> Show Orders for 4 27 2006 From 4 27 2006 To
Order Number	<input type="text"/>
Include Child Sub ID's	<input checked="" type="checkbox"/> Yes
<input type="button" value="View"/>	

- The report is displayed to the screen. Compare the "Trans ID" (transaction ID) from the RezStream Professional CC Processing report to the number displayed in the "Order ID" column to confirm transactions are listed correctly. Left-click the Order ID number to view more detail about the transaction.

Order Manager

Order ID	Date	Status	Amount
47121592	04/28/2006 14:21:11	Voided	\$3.40
47124397	04/28/2006 15:06:30	Completed	\$125.33
47124406	04/28/2006 15:07:23	Completed	\$99.09
47124417	04/28/2006 15:07:42	Completed	\$75.87

- Prior to sending the credit card batch, the transaction total from the RezStream Professional report should match the transaction total from the Online Merchant Center report. If discrepancies exist between the two systems, please contact either:
 - Credit Card Processing Support: First National Processing at 708-492-1030 (weekdays) or 800-920-9943 (weekends)
 - RezStream Support: 303-872-0220

CREDIT CARD PROCESSING – BEST PRACTICES

In this section, we will address some commonly asked credit card processing questions.

1. **What type of credit card processing account should I obtain?**

Transactions processed under a **lodging account** are eligible for the lowest credit card processing rates. **Retail accounts** are useful for businesses that take a majority of their payments prior to arrival or at check in.

2. **What is the difference between a *lodging* credit card account and a *retail* credit card account?**

Lodging accounts offer the lowest credit card processing rates because they are compliant with VISA and MasterCard credit card processing guidelines. In order to get the lowest rate, you must pre-authorize a guest's credit card at check in by swiping the card and using the Pre-Auth feature within RezStream Professional. You must then use the Post feature within RezStream Professional at check out. You may take advanced deposit payments, and other types of payments, with a lodging account, but the credit card rates are always higher for these types of payments. Lodging accounts are best for properties that want the absolute lowest rates and are willing to follow these guidelines to get the lowest rates.

Retail accounts are designed for non-lodging businesses or lodging businesses that take full payment in advance of the arrival date or at check in. Retail accounts do not offer rates as low as lodging accounts, but do offer lower rates than using a lodging account improperly.

Call RezStream at 866-360-8210 if you are not sure which type of account is best for your needs.

3. **If I have a lodging account am I *guaranteed* the lowest credit card processing rate?**

No. The mere possession of a lodging account does NOT guarantee the lowest credit card processing rate. In order to guarantee the lowest rate, transactions must be processed using the Hotel Pre-Auth and Post methods described on page 28 of this manual.

4. **What if my business requires partial or full payment prior to check in?**

If you must collect a partial or full payment prior to check in, your property may still want to use a lodging credit card processing account. For example, if you take a one night deposit in advance, but take the remainder of the payment at check out, you can still get lower rates on the final payment by using the Hotel Pre-Auth and Post option. However, if you take full payment in advance of the arrival date, or take all full payments at check in, you may be better off using a retail credit card processing account.

5. **What if my property records all payments prior to the guest's arrival *and* utilizes a *lodging account*?**

In this scenario, your property will be setting itself up to pay the highest credit card processing rates. Please note that RezStream strongly recommends either changing your deposit rules or applying for a **retail account**.

What happens to the guest's credit card when my property uses the *Hotel Pre-Auth* method?

During pre-authorization, a portion of the guest's credit limit is reserved to cover the expenses that will be incurred at your property. Although the guest's credit card is not charged until check out, the pre-authorized amount cannot be used elsewhere and can affect the guest's ability to use their credit card on another transaction.

For example, if the guest's credit card limit is \$500 (with a \$0 balance) and your property pre-authorizes \$350, the guest's credit card would be declined if another purchase exceeding \$150 is attempted.

6. When my front desk clerks are pre-authorizing a credit card, is it possible to authorize it for more than the room rate in order to cover incidental charges?

Yes. All VISA cards are automatically pre-authorized for 150% of the anticipated room charge. MasterCard and AMEX cards must be manually pre-authorized for an amount in excess of the room charge. VISA actually automatically pre-authorizes the card for 150% of whatever total amount is due on the invoice. Adding a higher pre-authorization amount is useful if the customer makes additional purchases during their stay.

7. When does the pre-authorization disappear from the guest's credit card?

The pre-authorized amount disappears from the guest's credit card when the amount becomes a real charge posted at check out, or typically, one week after the pre-authorization.

8. In order to prevent cards from being declined, should my property decrease the Address Verification Status (AVS) in the credit card gateway?

No. Although decreasing or disabling the AVS (see page 9) can reduce the number of declined credit card transactions, this will also increase your credit card processing rate.

CREDIT CARD SECURITY AND PCI COMPLIANCE INFORMATION

The payment card industry (PCI) has developed security standards for handling cardholder credit card information in a published standard called the PCI data security standard (DSS). These security requirements apply to all members, merchants, and service providers that store, process or transmit cardholder data.

So what does this mean to the average hospitality business? Banks, credit card processing gateways, software developers and even hospitality businesses must be PCI compliant. In fact, *any* business that processes credit cards is required to become PCI compliant. There are several levels of compliance depending on the number of credit card transactions a business processes per year. The good news is that it is relatively easy for hospitality businesses to get this type of certification.

How do hospitality businesses become PCI compliant? Here's a partial to do list to get you started:

- Use a validated software program and validated credit card gateway.
- Make sure you process all credit card payments on computers designated for business use only.
- You must maintain a basic firewall installation.
- Do not use default Windows passwords such as "password" to log into any computer.
- You must have anti-virus software installed on all computers and set to always scan.
- If you use a wireless network, you must also ensure that it is secure and encrypted.

In addition to these items, there are a few more requirements. You are also required to join a PCI compliance program that allows you to run security scans on your network. As part of this process, you will fill out a questionnaire that assesses your level of compliance before you can officially become PCI compliant.

All businesses who process credit cards must go through the PCI program, self test, submit to third party on-site testing (if required), and apply to be granted PCI compliance. **The deadline for all businesses to be PCI compliant is July 1, 2010.**

While PCI compliance may not be glamorous, it is critical to obtain with hackers and identity thieves out there who would like nothing more than to steal a few thousand of your customer's credit card numbers, and other private information, for their own personal gain.

The following areas must also be considered for proper implementation in a PCI compliant environment.

- Properly train and monitor admin personnel
- PCI compliant wireless settings
- Data transport encryption
- PCI compliant use of email

ACCESSING SENSITIVE CREDIT CARD DATA

Hospitality businesses are allowed to store credit card numbers and expiration dates for future use. However, all credit card numbers must be deleted after one year of storage. It is also recommended that you delete any card that you do not have a compelling reason to retain. (Need to retain for an advance booking payment)

It is never permissible to store credit card swiped data or security codes (the three and four digit numbers on the back of credit cards). Although you are allowed to store numbers, there are certain requirements to follow such as strong credit card encryption.

RezStream includes the following credit card number storage protections within RezStream Professional and the RezStream Booking Engine:

- RezStream does not store swiped data from any credit card.
- RezStream uses SSL (secure socket layer) and strong encryption when transferring online credit card numbers.
- RezStream does not store security codes or transfer security codes.
- RezStream enforces "strong passwords" to access the system and any related credit card processing features. Passwords are automatically reset every 90 days. All strong

- passwords must be 7-10 characters and contain one upper case character, and at least one special character (number or unique character)
- RezStream does not display full card numbers (Primary Account Numbers PAN) on invoices, in letters, etc.
 - Full credit card numbers cannot be viewed without entering a user name and password.
 - RezStream logs all cc processing related activities.
 - RezStream provides mechanisms to delete individual credit card numbers and also aggregate credit card data.

CREDIT CARD STORAGE METHODS

RezStream Professional and the RezStream Booking Engine do not store any magnetic stripe data, card validation codes, or PIN blocks. All credit card numbers stored within RezStream Professional are encrypted with 256-bit strong encryption and the entire credit card number is only displayed when a merchant has an impending need to use the credit card number and uses a password to access this data.

CREDIT CARD PASSWORD ACCESS

The PCI standard requires the following password complexity for compliance (often referred to as using “strong passwords”):

- Passwords must be at least 7-10 characters
- Passwords must include both upper case, lower case, numeric and alphabetic characters
- Passwords must be changed at least every 90 days

PCI user account requirements beyond uniqueness and password complexity are listed below:

- If an incorrect password is provided 5 times the account should be locked out
- Account lock out duration should be at least 30 mins. (or until an administrator resets it)
- Do not use group, shared, or generic user accounts

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant.

PROPERLY TRAIN AND MONITOR ADMINISTRATIVE PERSONNEL

It is your responsibility to institute proper personnel management techniques for allowing admin user access to credit cards, site data, etc. You can control whether each individual admin user can see credit cards (or only last 4).

In most systems, security breach is the result of unethical personnel. Pay special attention to whom you trust into your admin site and who you allow to view full decrypted payment information.

PCI COMPLAINT REMOTE ACCESS

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

If users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP)/Terminal Server, pcAnywhere, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for pcAnywhere it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software
- Allow connections only from specific IP and/or MAC addresses
- Use strong passwords for logins
- Enable encrypted data transmission
- Enable account lockouts after a certain number of failed login attempts
- Require that remote access take place over a VPN as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Revoke access as soon as the support task is completed

PCI COMPLIANT WIRELESS NETWORKS

The PCI standard requires the encryption of cardholder data transmitted over wireless connections. The following items identify the PCI standard requirements for wireless connectivity to the payment environment:

- Firewall/port filtering services should be placed between wireless access points and the payment application environment with rules restricting access
- Use of appropriate encryption mechanisms such as VPN, SSL/TPS at 128 bit, WEP at 128 bit, and/or WPA
- If WEP is used the following additional requirements must be met:
 - Another encryption methodology must be used to protect cardholder data
 - If automated WEP key rotation is implemented key change should occur every ten to thirty minutes
 - If automated key change is not used, keys should be manually changed at least quarterly and when key personnel leave the organization
- Vendor supplied defaults (administrator username/password, SSID, and SNMP community values) should be changed
- Access point should restrict access to known authorized devices (using MAC Address filtering)

If you install Payment Application into a wireless environment, use compliant wireless settings, per PCI Data Security Standard 1.3.9, 2.1.1 and 4.1.1:

1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)
- Rotate shared WEP keys whenever there are changes in personnel with access to keys
- Restrict access based on media access code (MAC) address

NETWORK SEGMENTATION (FIREWALL PROTECTION)

The PCI standard requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

MAINTAIN AN INFORMATION SECURITY PROGRAM

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI compliance requirements in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and

- perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
 - Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
 - **Call in outside experts as needed.**

There is no such thing as partial PCI compliance

There are many businesses that mistakenly think they will be compliant if they simply do the things on the PCI compliance list. Doing these things does not make a business PCI compliant. You must also go through the PCI program, self test, submit to third party on-site testing, and apply and be granted for PCI compliance.

Who do I contact to become PCI compliant?

You should contact your merchant account provider regarding PCI compliance. Most merchant account providers have PCI compliance programs and can help you complete the process. Call RezStream at 866-360-8210 for more information or call your local merchant account provider.

REZSTREAM CONTACT INFORMATION

For additional information on any of the topics contained in this manual, please contact:

RezStream Help Desk: 303-872-0220

Please contact RezStream sales at 866-360-8210 for information on RezStream add-on modules, including:

- RezStream Booking Engine
- Call Accounting
- Credit Card Processing

Normal business hours are 8:00AM to 5:00PM, Monday through Friday, MST.

After hours support is available for an additional fee.

RezStream, Inc.
2601 Blake Street, Suite 10
Denver, CO 80205
Sales: 866-360-8210
Support: 303-872-0220
Fax: 303-297-3233
www.rezstream.com
sales@rezstream.com
support@rezstream.com