

# Introduction

1

## In This Chapter

What is **VersiTouch Credit Access?**, 1-1

**VersiTouch Credit Access** Features, 1-2

Who Should Read This Manual, 1-2

Where to Find More Information, 1-2

**VersiTouch Credit Access** is a utility that will help you achieve PCI DSS compliance. It allows authorized users to view protected credit card information, manually generate force files, and/or to remove sensitive credit data when it's no longer needed for business purposes. You should refer to the **VersiTouch PA-DSS Implementation Guide** for our recommendations on implementing and maintaining a PCI compliant point of sale solution. Read on for more information about the **VersiTouch Credit Access** solution.

This manual is designed to:

- Act as a guide through the **VersiTouch Credit Access** installation process.
- Illustrate how **VersiTouch Credit Access** operates.
- Help solve problems that can arise during normal operation of **VersiTouch Credit Access**.

## What is **VersiTouch Credit Access**

**VersiTouch Credit Access** is a utility that provides Payment Card Industry (PCI) Payment Application – Data Security Standard (PA-DSS) compliant access to credit card data that has been processed by a **VersiTouch Point of Sale (POS)** terminal via **VersiTouch Credit**. **VersiTouch Credit Access** allows you to correct problems that may have occurred during POS operation and to help bring the merchant into compliance with the PCI-DSS.

## Who Should Read This Manual?

This **VersiTouch Credit Access** Manual is a guide to the installation and operation of **VersiTouch Credit Access**, version 10.10.22. Any person actively involved in the training, installation, or maintenance of **VersiTouch Credit** should use this manual. This manual is not required for general operation of **VersiTouch Credit** when used in conjunction with the **VersiTouch POS** system.

## Where to Find More Information

For additional information about **VersiTouch Credit**, or any of the other software products in the **VersiTouch** product line, contact your nearest authorized VersiTouch reseller or visit the **VersiTouch** website at <http://www.versitouch.com>. Registered website users will find instruction sheets, PCI compliance references, and program updates for all of the **VersiTouch** software products, including **VersiTouch Gift Card** and the **VersiTouch Hotel** Property Management System interface.

### **VersiTouch Credit Access Features**

User Access management features that meet PCI PA-DSS standards.

Comprehensive logs to track user access to sensitive credit card data.

Features that securely remove sensitive credit card data when no longer required for business purposes.

Disaster recovery for failed batches.

## INFORMATION

**VersiTouch Credit** is sometimes referred to as **VersiCredit**, a reference to the main program filename with the .exe extension truncated. This method of abbreviation is common for all **VersiTouch** products.

# Installation

## 2

### In This Chapter

Preparing to Install **VersiTouch Credit Access**, 2-1

Installing **VersiTouch Credit Access** 2-3

Installing License Key Drivers, 2-4

### Preparing to Install **VersiTouch Credit Access**

The **VersiTouch Credit Access** software must be installed on the **VersiTouch POS** fileserver. In order to activate **VersiTouch Credit Access**, a license key registered to the merchant for either **VersiTouch POS** or **VersiTouch Credit** must be installed on the PC that you intend to use to run the program.

What follows is a list of items that are required during the installation in order for **VersiTouch Credit Access** to function properly. More detail about each of these items is provided later in the manual.

- Access to the fileserver PC.
- **VersiTouch Install CD**, v10.10.22 or later.

## Where to Install *VersiTouch* Credit

***VersiTouch* Credit Access** must operate on the PC that operates ***VersiTouch* Credit**.

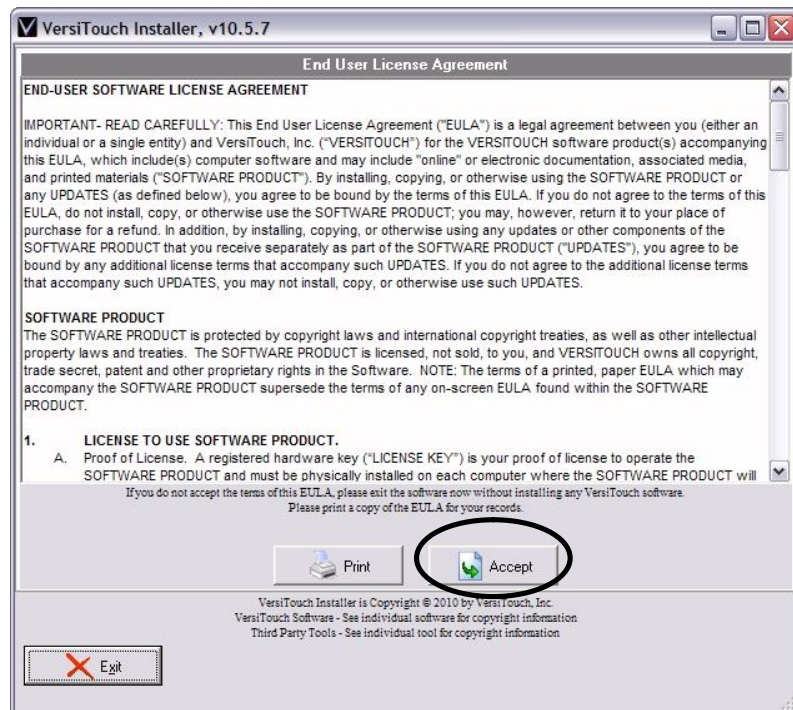
Troubleshooting is usually easier if all *VersiTouch* programs are installed onto a single dedicated fileservers PC.

## Installing ***VersiTouch* Credit Access**

Insert the ***VersiTouch* Install CD** into the CD-ROM of the ***VersiTouch* POS** fileserver. Installing the software across a network connection is not recommended.

The *VersiTouch* End-User License Agreement (EULA) will appear in a window, similar to the example shown in Figure 2-1.

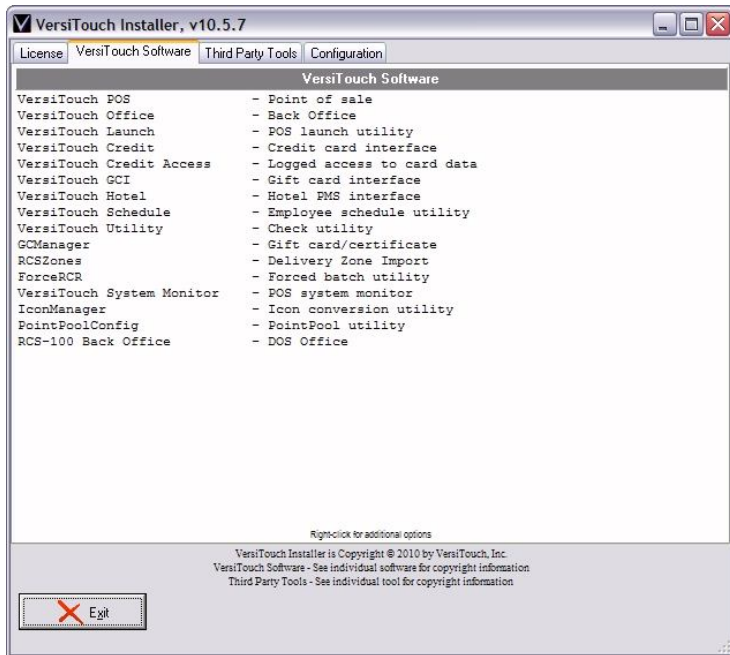
Figure 2-1. *VersiTouch* Installer, EULA Screen Example.



Click on the **Accept** button after reading the EULA.

The screen will automatically switch to the VersiTouch Software list after you accept the terms of the EULA.

Figure 2-2. VersiTouch Installer, VersiTouch Software Tab.



Select **VersiTouch Credit Access** from the list and then click on the **Install Selected** button. Input the letter of the hard drive on which you want to install the new **VersiTouch Credit Access** utility. If you're working from the POS fileserver, this will typically be "C".

Figure 2-3. Where to install VersiTouch Credit Access.



## Current License Key Types

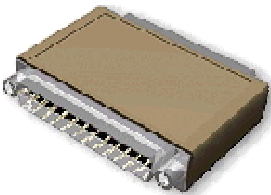
Hasp



Hasp (USB)



Key-Lok



Key-Lok (USB)



Rainbow



## Selecting a VersiTouch License for Activation

Before you can activate **VersiTouch Credit Access**, you must first identify a valid **VersiTouch POS** or **VersiTouch Credit** license to associate with the activation. **VersiTouch Credit Access** is designed to operate across a network connection at either a point of sale terminal station or the PC that runs **VersiTouch Credit** (it's possible that **VersiTouch Credit** runs on a POS terminal but that would be an uncommon situation).

# Activation

## 3

### In This Chapter

**VersiTouch Credit Access** Activation, 3-2

**VersiTouch Credit Access** Primary Administrator, 3-3

In this chapter, we'll be discussing the process of activating the **VersiTouch Credit Access** software and creating a primary administrator.

### Preparing to Activate **VersiTouch Credit Access**

What follows is a list of items that are required during the installation in order for **VersiTouch Credit Access** to function properly. More detail about each of these items is provided later in the manual.

- Network access to the **VersiTouch POS** fileserver.
- Access to a PC that has either a valid **VersiTouch Credit** or **VersiTouch POS** software license key installed.
- A completed **VersiTouch Credit Access** Authorization form.

### IMPORTANT

1. **VersiTouch Credit Access** must be installed in the RCS folder on the shared drive of the POS fileserver.
2. **VersiTouch Credit Access** must be activated with a valid **VersiTouch Credit** or **VersiTouch POS** site ID prior to use.
3. If a merchant has different site IDs for **VersiTouch Credit** and **POS**, only one site ID can be used with **VersiTouch Credit Access**. **VersiTouch Credit** is recommended.
4. **VersiTouch Credit Access** will only operate on PCs with matching site IDs.

## Activating *VersiTouch* Credit Access

In order to activate ***VersiTouch* Credit Access**, the identity of the primary administrator must be verified before we will issue an activation code. The primary administrator can verify their identity by either a notary public or by having his/her identity verified by the installing reseller. The required form can be found in the back of this manual in Appendix A. Once the form is complete, mail the original signed copy to:

VersiTouch, Inc.  
ATTN: VCA Auth  
6019 SE 44<sup>th</sup> Avenue  
Portland, OR 97206

Read through this manual for directions and illustrations about the various features of ***VersiTouch* Credit Access**. After you've familiarized yourself with the general layout of the screens, follow the steps below to activate ***VersiTouch* Credit Access**:

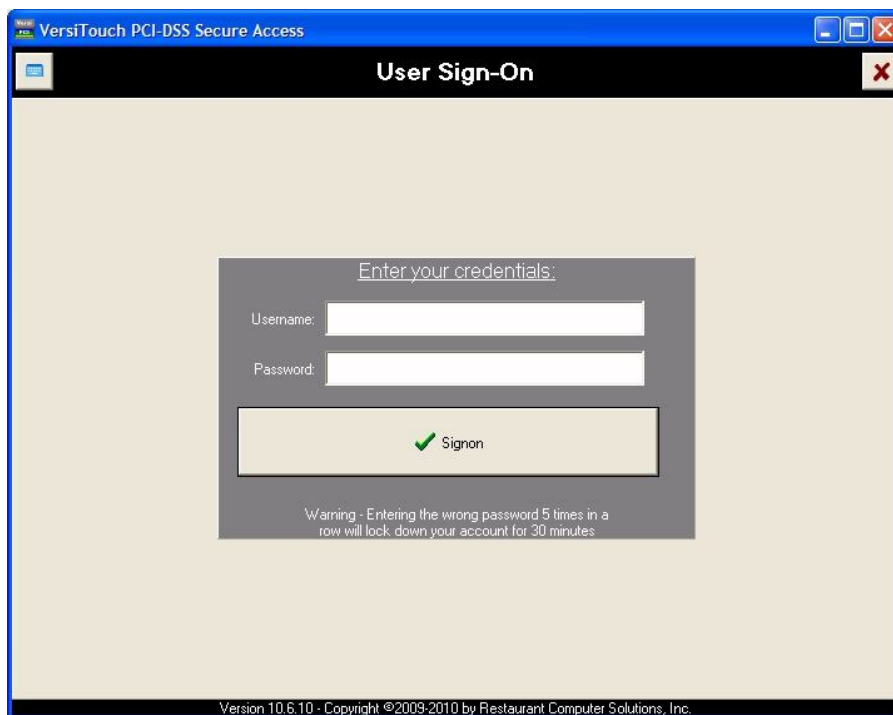
1. Start ***VersiTouch* Credit Access** from one of the following locations:
  - a. A POS terminal, by clicking on **Managers** from the POS main screen, then selecting **Credit Transactions**.
  - b. The fileserver (if it has a valid ***VersiTouch* POS** or ***VersiTouch* Credit** license installed), by double-clicking the ***VersiTouch* Credit Access** icon located on the desktop.
  - c. The PC that runs *VersiTouch* Credit. You may need to create a shortcut on the desktop that links to the program executable file found on the shared drive of the fileserver.  
(for example: i:\rcs\versicreditaccountaccess.exe)
2. Contact ***VersiTouch, Inc.*** during business hours (Monday-Friday, 9 AM to 5 PM PST) at 1-800-655-7349.
3. After reading the site ID code to the ***VersiTouch*** representative, you will receive an activation code.
4. Enter the activation code in ***VersiTouch* Credit Access**.

While on the phone with the *VersiTouch* representative, you should proceed immediately to the next phase to create a primary administrator.

Login using a temporary **VersiTouch** admin account that the **VersiTouch** representative will provide.

### Activate the temporary admin

5. Read the revised site ID code to the **VersiTouch** representative, who will generate a temporary admin activation code.
6. Enter the temporary admin activation code in **VersiTouch Credit Access**.
7. Create a new user to be your permanent Administrator with all functions enabled.
8. Logout the temporary **VersiTouch** Administrator.
9. Login using the permanent Administrator.



10. Create additional users on a business need-to-know basis.
11. Remove old restricted data from the POS system.
12. Review Access logs daily for employee access to restricted data.

# Operation

# 4

## In This Chapter

Select Actions Screen,  
4-2

Menu Bar, 4-3

Manage Users, 4-4

View Access Log, 4-8

View Transactions, 4-9

Generate Batch Force  
File, 4-11

Delete PCI Data, 4-13

Encryption keys, 4-16

In this chapter, we'll be discussing the various features and screens of the **VersiTouch Credit Access** software.

## Primary Features of the Main Screen

*Title Bar* - Shows the program title.

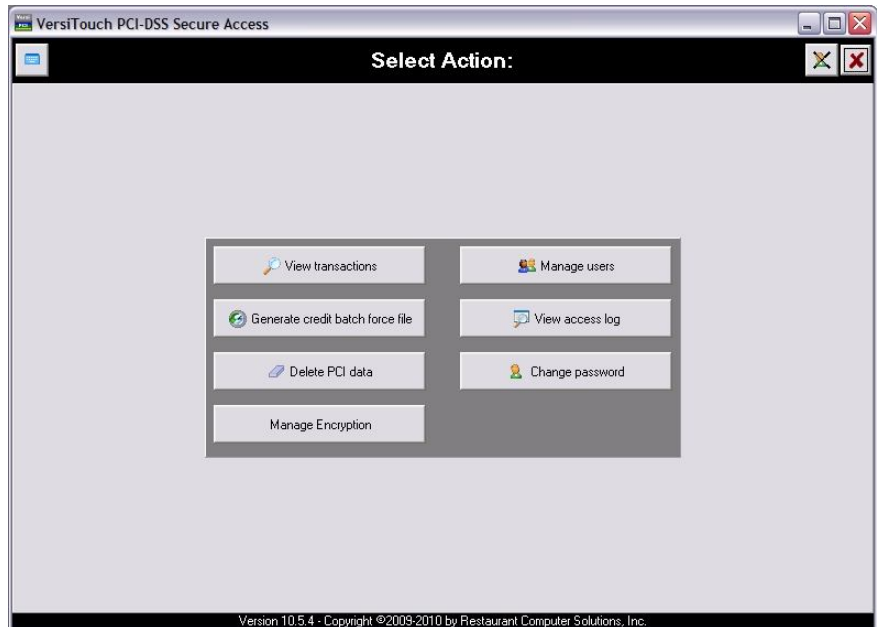
*Window Buttons* - Minimize, maximize, or close the window.

*Menu Bar* – the **VersiTouch Credit Access** is primarily used when the program is running on a touchscreen monitor.

*Action Buttons* – the primary navigation tool for accessing the features of **VersiTouch Credit Access**.

The Select Action screen, shown in Figure 4-1, is the main menu for **VersiTouch Credit Access**.

Figure 4-1. VersiTouch Credit Access, Main Select Action Screen.



There are six primary actions available on the Select Action screen: **View Transactions**, **Generate Credit, Batch Force File**, **Delete PCI Data**, **Manage Users**, **View Access Log**, **Change Password**, and **Manage Encryption**. These actions will be discussed in the order in which they are typically used, beginning with **Manage Users**.

## Menu Bar Elements

*Keyboard* – enable an onscreen keyboard, if using a touchscreen.

*Back* – returns you to the previous screen.

*Logout* – log the current user out of **VersiTouch Credit Access** without exiting the program.

*Exit* – shut down the **VersiTouch Credit Access** program.


## VersiTouch Credit Access Menu Bar


The **VersiTouch Credit Access** Menu Bar provides touchscreen navigation options. The Menu Bar has three basic elements, as summarized below.


The menu bar at the top of the “Select Action” screen has three actions.


Figure 4-2. VersiTouch Credit Access menu bar.



The keyboard icon () will enable the onscreen keyboard.

Second from the right is an icon that has a person with an “x” over it () , this will log out the current user, but will leave **VersiTouch Credit Access** open.

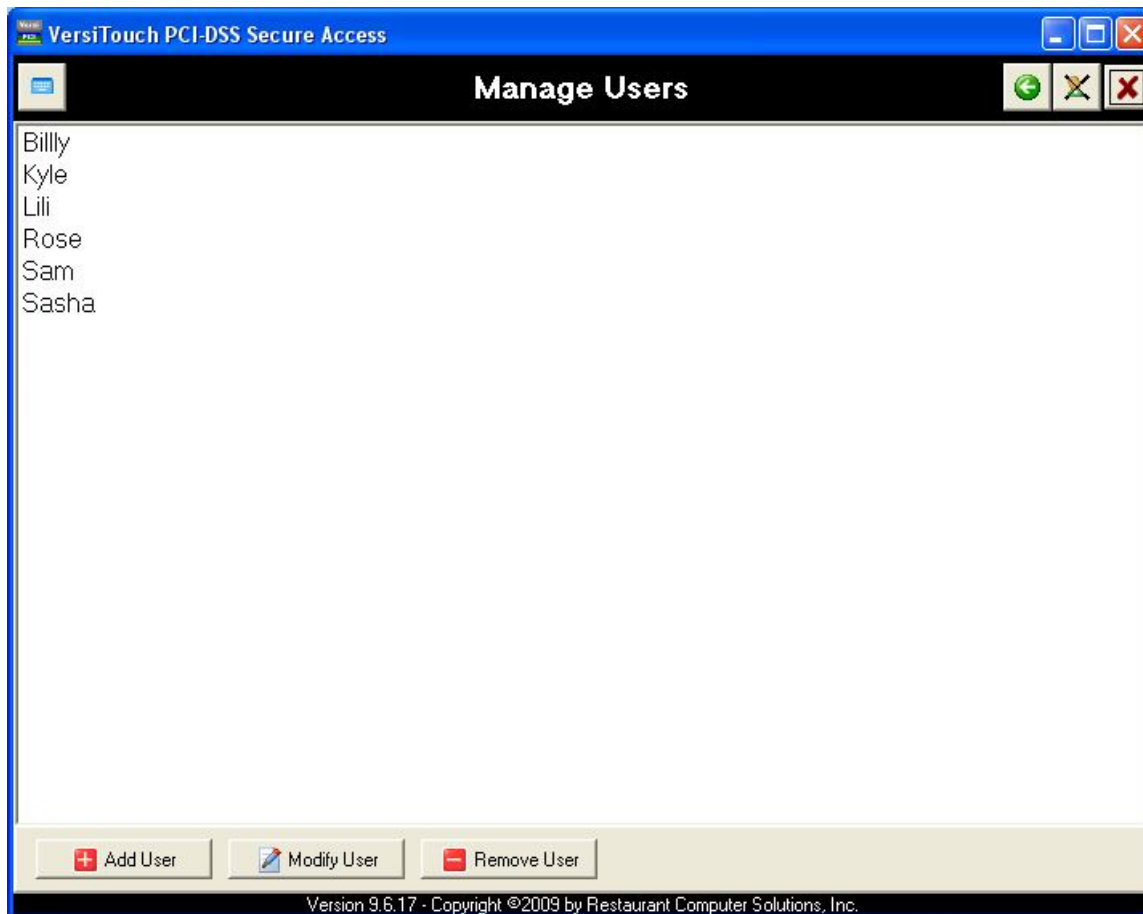
On the far right is an “x” icon () that will close VersiTouch Credit Access.

When you navigate from the main “Select Action” screen an icon with a green arrow () appears next to the logout function. This button will allow you to go back to the previous screen.

## Manage Users

Access the “Manage Users” screen by clicking the **Manage User** button. Once at the “Manage User” screen, there are three buttons along the bottom of the screen: **Add User**, **Modify User** and **Remove User** (Figure 4-3)

Figure 4-3. Manage Users Menu



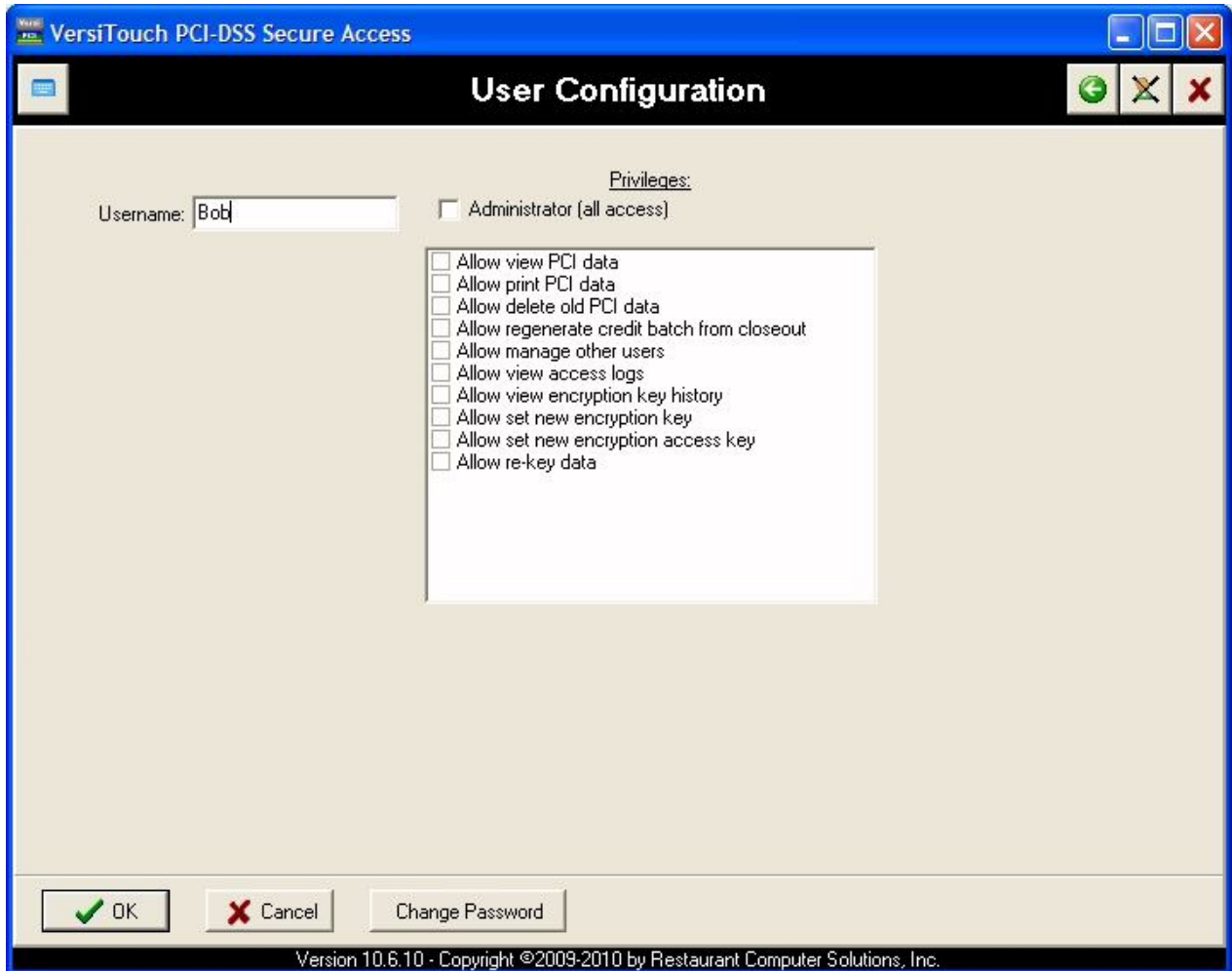
You must not use group, shared, or generic accounts; all users must have a unique ID. Accounts become locked after 5 failed attempts to login and you must wait 30 minutes before trying again.

If a user account is inactive for 15-minutes, the user is logged out and must re-enter their user ID and password to access any functions in VersiTouch Credit Access.

## Add User

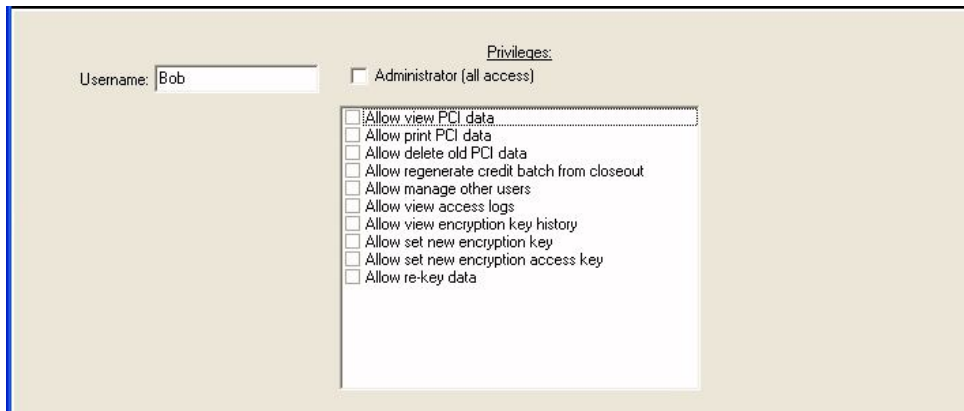
To add a user, click the **Add User** button. The words “User Configuration” will run across the top of the new window. The **OK**, **Cancel**, and **Set Password** buttons will run along the bottom of the window (Figure 4-4).

Figure 4-4. Clicking on the Add User button will open the “User Configuration” screen.



Enter the new user's name in the box to the right of "Username". Then select which function(s) of **VersiTouch Credit Access** the new user will be able to utilize. This is done by clicking the boxes next to the various privileges available on **VersiTouch Credit Access** (Figure 4-5).

Figure 4-5. Entering a new user's name and selecting privileges.



The screenshot shows a web interface for creating a user. On the left, there is a text input field labeled "Username:" containing the text "Bob". To the right, under the heading "Privileges:", there is a checkbox labeled "Administrator (all access)". Below this, a scrollable list of checkboxes is displayed, each with a corresponding privilege name:

- Allow view PCI data
- Allow print PCI data
- Allow delete old PCI data
- Allow regenerate credit batch from closeout
- Allow manage other users
- Allow view access logs
- Allow view encryption key history
- Allow set new encryption key
- Allow set new encryption access key
- Allow re-key data

The PA-DSS recommends splitting the knowledge of the encryption key assigned to your data and the key used to access the data key. You should assign only one person the privilege to "Allow set new encryption key" and a separate person to "Allow set new encryption access key". There is a key custodian form, available at the end of this *User Guide*, that each of those key custodians should sign.

Finally choose a password by clicking on **Set Password**, using the rules shown in Figure 4-6.

Figure 4-6. Change Password Screen



The screenshot shows a "Change Password" screen. At the top, the title "Change Password" is displayed in white on a black background. Below the title, the heading "PCI-DSS password rules" is shown. Underneath, the text "Your password:" is followed by a list of requirements:

- must have 7 or more characters
- must include an uppercase letter
- must include a lowercase letter
- must include a numeral or punctuation character
- cannot be the same as any of the previous 4 passwords
- must be changed every 90 days or less

At the bottom of the screen, there are two input fields. The first is labeled "New password:" and contains a series of asterisks. The second is labeled "Re-enter new password:" and also contains a series of asterisks.

Click on **OK** to save the new user. The screen will return to the “Manage Users” screen (Figure 4-3) with the new user included in the list.

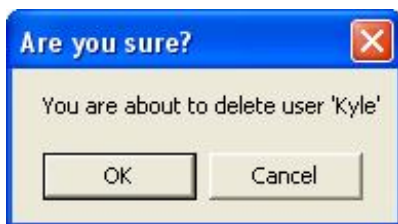
### Modify User

On the “Modify User” screen, you can change the privileges, password and name of the user by following the same instructions as “Adding Users”.

### Remove User

Select a user from the list of the “Manage Users” screen. Click on **Remove User** and a box will appear to confirm that you want to remove the selected user. If you have selected the correct user to delete, click the **OK** button (Figure 5).

Figure 4-7. Delete User Confirmation



## IMPORTANT

Per the PCI-DSS, you are strongly advised to immediately remove users that are no longer employed or associated with your business.

## View Access Log

Select **View Access Log** from the “Select Action” screen. The “View Access Log” allows a user to view which features any user has accessed via **VersiTouch Credit Access**. There are three different filters that will allow a user to view specific data: “Start Dates” and “End Dates”, “User Types” and “Access Type”.

Figure 4-8. The filters in the View Access Log menu.

Start Date: 9/24/2009  
End Date: 10/ 1/2009  
View Access Log

Filter by users:  
 Lili  
 Rose  
 Sam  
 Sasha  
 Stockton

Filter by access type:  
 Sign on  
 Force file Generation  
 User management  
 Change password  
 View PCI restricted data  
 View transactions (no PC)

Once the filters have been set, click on the **View Access Log** button, then all of the filtered information will be displayed in the window below as in Figure 4-9.

Figure 4-9. Example of the Access Log.

VersiTouch PCI-DSS Secure Access  
Access Log

Start Date: 4/30/2010  
End Date: 5/ 7/2010  
View Access Log

Filter by users:  
 Jon

Filter by access type:  
 Sign on  
 Force file Generation  
 User management  
 Change password  
 View PCI restricted data  
 View transactions (no PC)  
 Manage encryption

Username	Date/Time	Access
VersiTouchAdmin	2010-05-07 11:16:40	Signon
VersiTouchAdmin	2010-05-07 11:16:41	Validating for initial Administrator
VersiTouchAdmin	2010-05-07 11:17:59	Accessing 'Manage users' function
VersiTouchAdmin	2010-05-07 11:18:26	Creating new user 'Jon'
Jon	2010-05-07 11:18:26	New user created by 'VersiTouchAdmin'
VersiTouchAdmin	2010-05-07 11:18:32	Updating user 'Jon'
Jon	2010-05-07 11:18:32	User record updated by 'VersiTouchAdmin'
VersiTouchAdmin	2010-05-07 11:18:35	Signoff
Jon	2010-05-07 11:18:42	Signon
Jon	2010-05-07 11:18:53	Accessing 'Manage encryption' function
Jon	2010-05-07 11:19:28	Accessing 'View access log' function

Version 10.5.4 - Copyright ©2009-2010 by Restaurant Computer Solutions, Inc.

VersiTouch Credit Access logging is enabled upon startup and cannot be disabled. It logs the following information for access to sensitive PCI data:

Access types, including:

- All invalid logical access attempts
- Actions taken by users, including login/out
- Addition, deletion, or modification of users and their assigned functions
- Access to decrypted cardholder data
- Removal of sensitive PCI data from daily storage files
- Access to audit trails
- Changes to encryption keys

Entries include:

- User identification
- Date and time of each event
- Type of access with success or failure indication

The VersiTouch Credit Access log is contained within a private database and is located on the POS fileserver in “C:\RCS\VCA\DATA\CAADATA.DTA”.

For PA-DSS compliance, log files must have access controls applied so that only authorized users can modify them. Additionally, the Windows Security Event Log will need to be configured to log access to the VersiTouch Credit Access log files. A review of both the Windows Security Event Log and the VersiTouch Credit Access log files will give you a clear picture which details when files have been modified or removed from the system.

## IMPORTANT

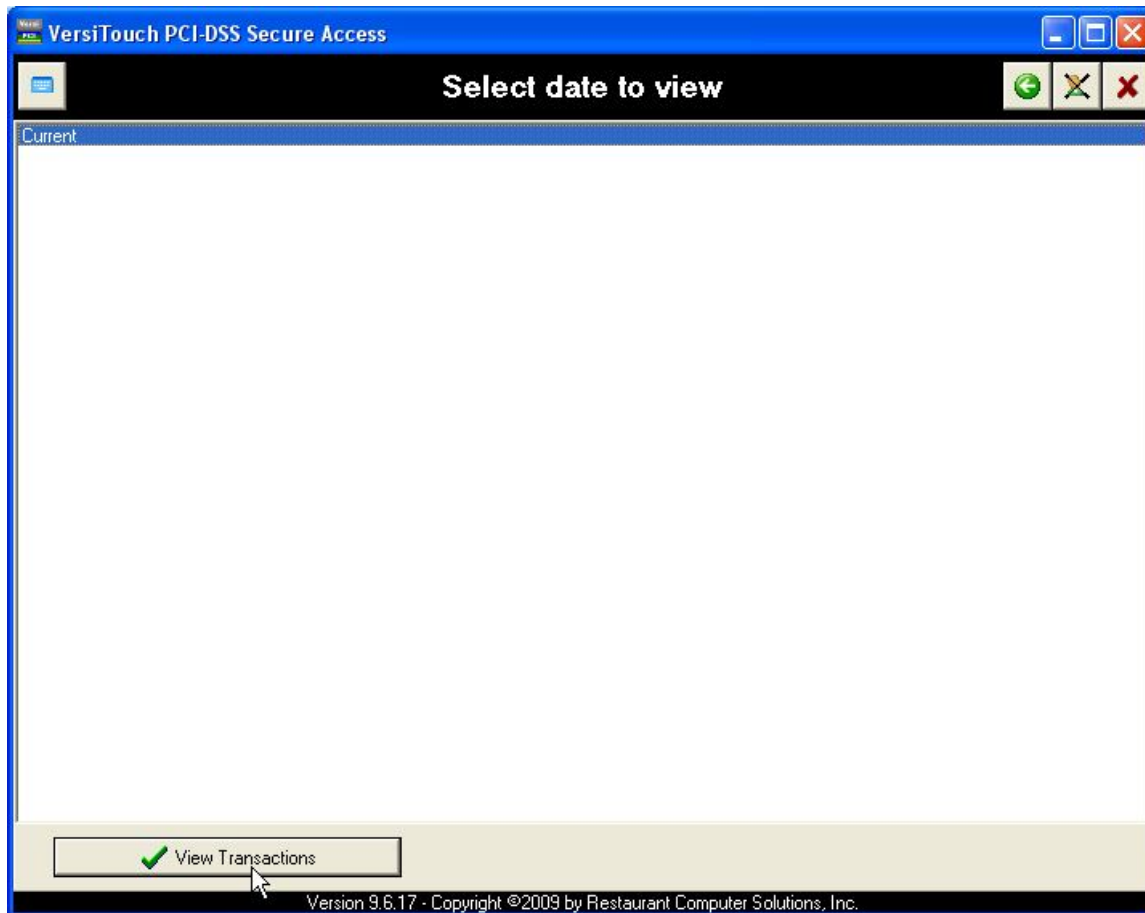
You are strongly advised to review these logs on a daily basis and to question all access to restricted data. The data contained in this log will allow you to recreate the actions performed by a user.

## View Transactions

Click the **View Transactions** button on the “Select Action” screen to view the transactions for a specified day.

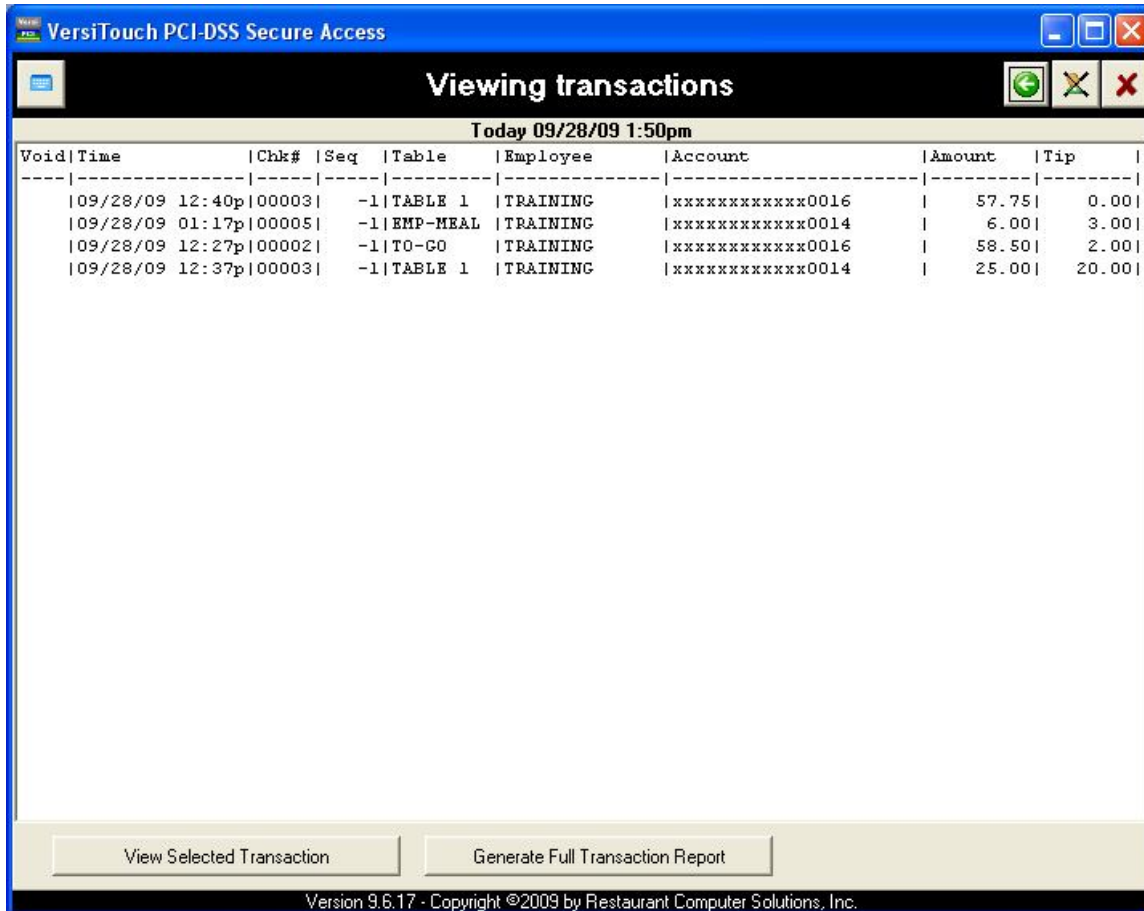
First select the current day’s credit transactions or the date you want to view. Then click **View Transactions** on the bottom left of the screen (Figure 4-10).

Figure 4-10. View Transactions Screen



This will display the credit transactions without showing protected information as shown in Figure 4-11 (i.e. account numbers, expiration dates, cardholder's name).

Figure 4-11. Viewing transactions without protected data



There are two options once the transactions are on the screen. It is possible to view the protected information for a specific card holder or for the entire day's credit transactions.

1. The **View Selected Transaction** option will show all of the protected information for a single credit transaction.
2. The **Generate Full Transaction Report** option allows the user to view protected credit card information.

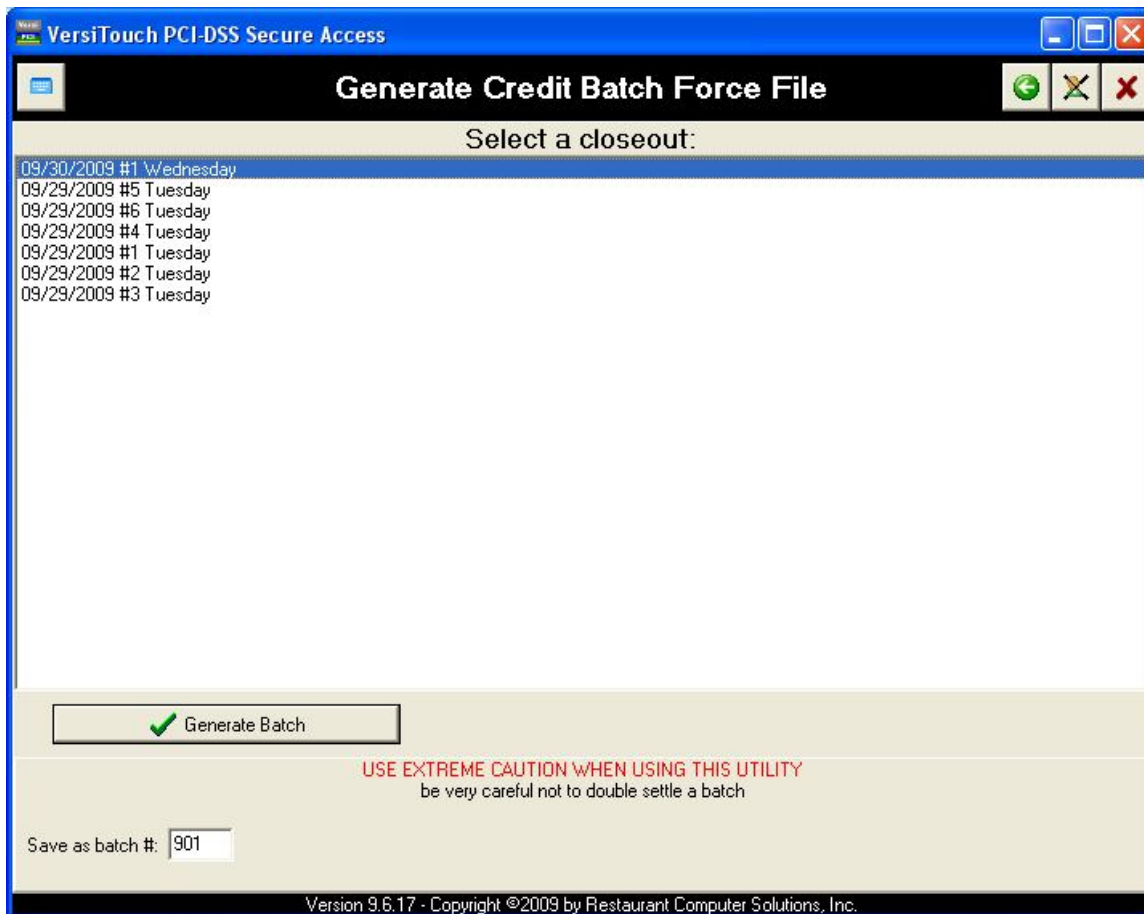
The user will have the option of printing this information by clicking the **Print Transaction** button that will appear on the bottom left of the screen.

## Generate Batch Force File

This function allows a user to generate a replacement batch for processing when closing credit transactions at the end of the business day.

To do this, highlight the day's closeout to batch. Type in the number you would like to save the batch in the box to the right of "Save as batch #". Then click on the **Generate Batch** button on the bottom left of the screen (Figure 4-12).

Figure 4-12. Selecting a closeout to generate a replacement batch.

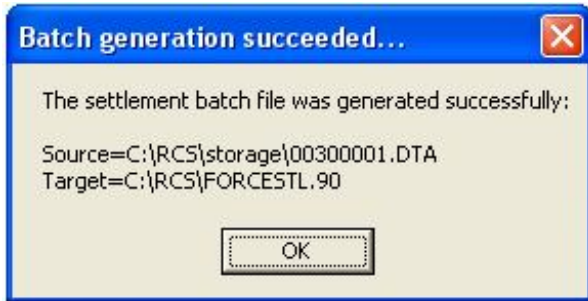


### IMPORTANT

Exercise extreme caution when using this function! You could very easily double charge your customers. Contact your credit card provider to verify a deposit before generating a replacement batch force file. Refer to "Troubleshooting" in Chapter 5 for more detail on settling a forced batch.

If the force batch creation was successful, a screen similar to the one in Figure 4-13 will pop up. Click **OK** to continue.

Figure 4-13.



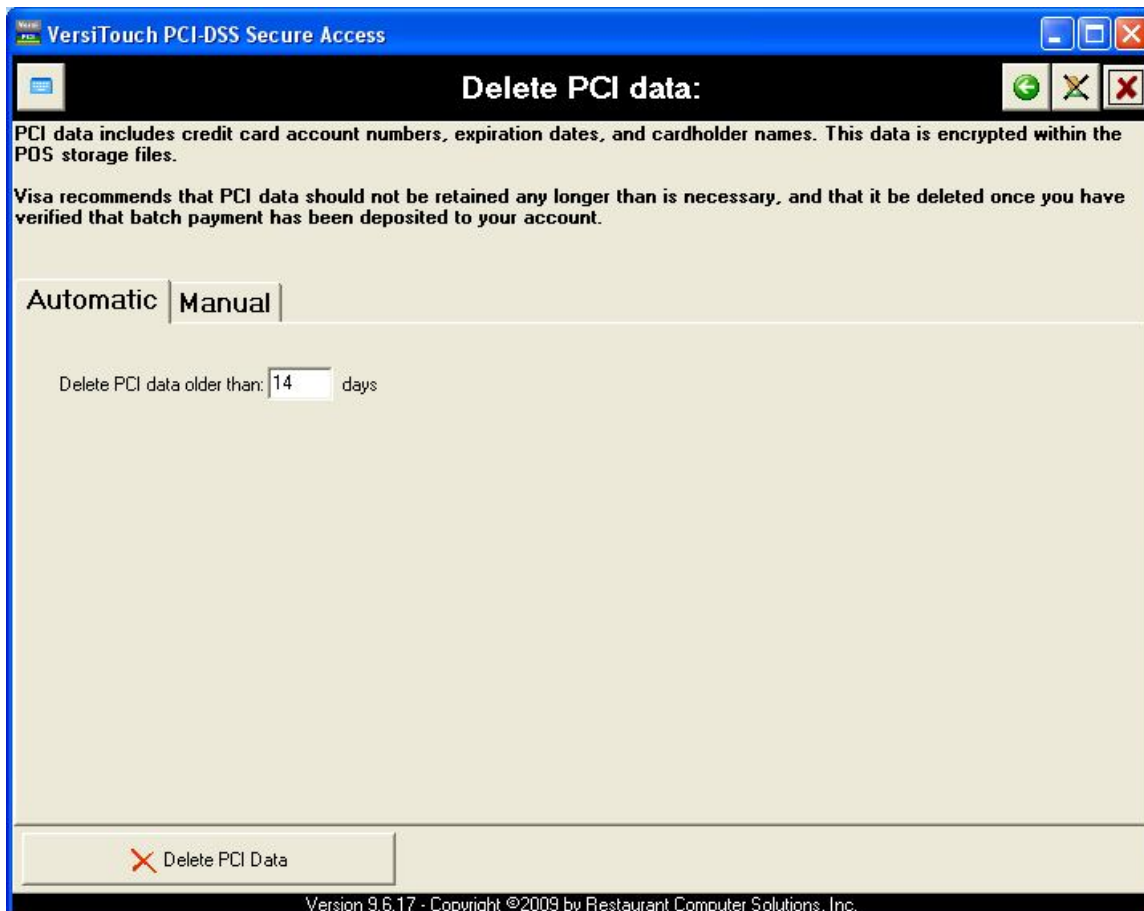
## Delete PCI Data

PCI is an acronym for Payment Card Industry. The Payment Card Industry has mandated that certain types of data found on credit cards must be protected by merchants and their payment applications. Personal information about a credit card holder, including their name, primary account number, and expiration date, must be secured. The best way to deal with this information is to delete it after you have no further business reason to retain it (typically, after confirmation of payment to your account is received).

There are two options once you access the Delete PCI data menu. PCI data can either be deleted automatically by deciding how many days you want to keep the data. Another way is to delete the data manually on a per day basis.

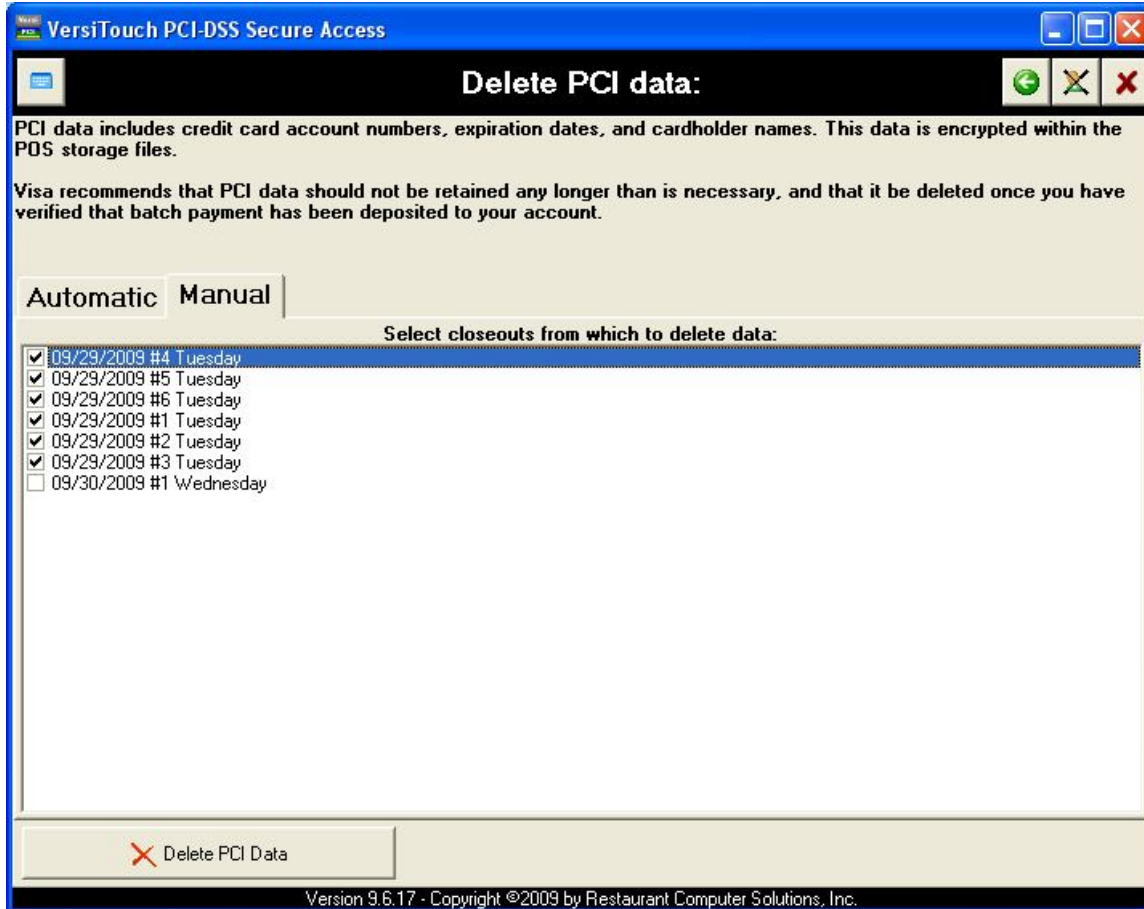
Figure 4-14 shows the screen that allows PCI data to be deleted automatically. To do this, in the box next to where it says “Delete PCI Data Older Than:” enter the number of days you would like to **keep** the data.

Figure 4-14. Automatically delete PCI data



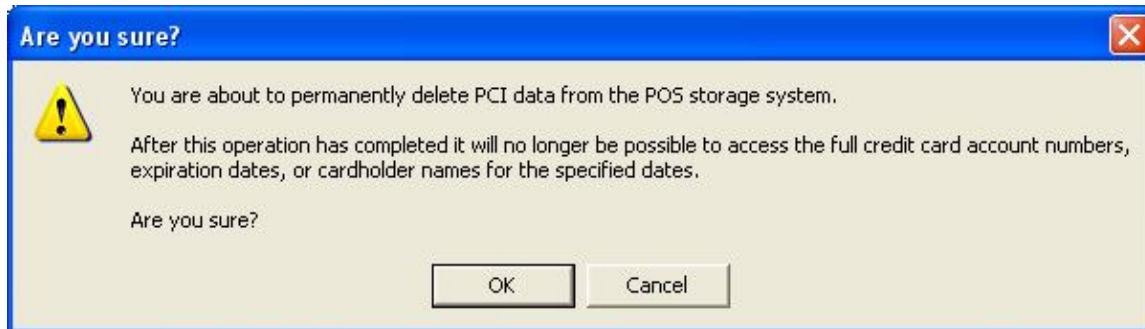
To delete specific data, click on the tab that is labeled “Manual”. First check the box next to the day(s) you want to delete.

Figure 4-15. Manually selecting data to be deleted.



After clicking **Delete PCI**, a screen will appear warning that card holder names, card numbers, and expiration dates will be deleted, like the one in Figure 4-15. Once you've clicked **OK**, another screen will appear that confirms the data has been deleted.

Figure 4-16. Warning before proceeding with deleting PCI data.



Refer to **Troubleshooting** in Chapter 5 if you encounter problems with the deletion process.

## Manage Encryption Settings

Access the “Manage Encryption Settings” screen by clicking the **Manage Encryption** button. Once at the “Manage Encryption Settings” screen, there are three tabs along the bottom of the screen: **Encryption Keys** (Figure 4-17), **Encryption Access Key** (Figure 4-18) and **Re-Key Existing Data** (Figure 4-19).

**VersiTouch Credit Access** generates strong encryption keys from a user supplied key via 128-bit AES. The keys are managed and stored separately in a securely encrypted format and signed to the data files. Any changes to key storage will result in detection and the program will then invalidate all access to key storage. You must change your encryption keys *at least* on an annual basis or at any point that you suspect the keys may have been compromised. After changing keys, you should immediately re-key any existing sensitive PCI data that may still be stored in the daily closeout files to revoke the old keys.

As noted in the **User Configuration** section of this manual, the PA-DSS recommends split knowledge of keys and that the key custodians sign a form specifying that they understand and accept their key-custodian responsibilities. A copy of the custodian form can be found at the end of this *User Guide* or on our website, <http://www.versitouch.com>.

Knowledge of encryption keys should be split between two users. In addition, the PCI PA-DSS requires the encryption access key to be stored on a separate server or memory device, such as the hard drive in another PC on the network or a USB thumb drive. Any PCs that run VersiTouch POS, VersiTouch Credit, VersiTouch Office, or VersiTouch Credit Access must have continuous access to this location.

Figure 4-17. Manage Encryption Settings Screen

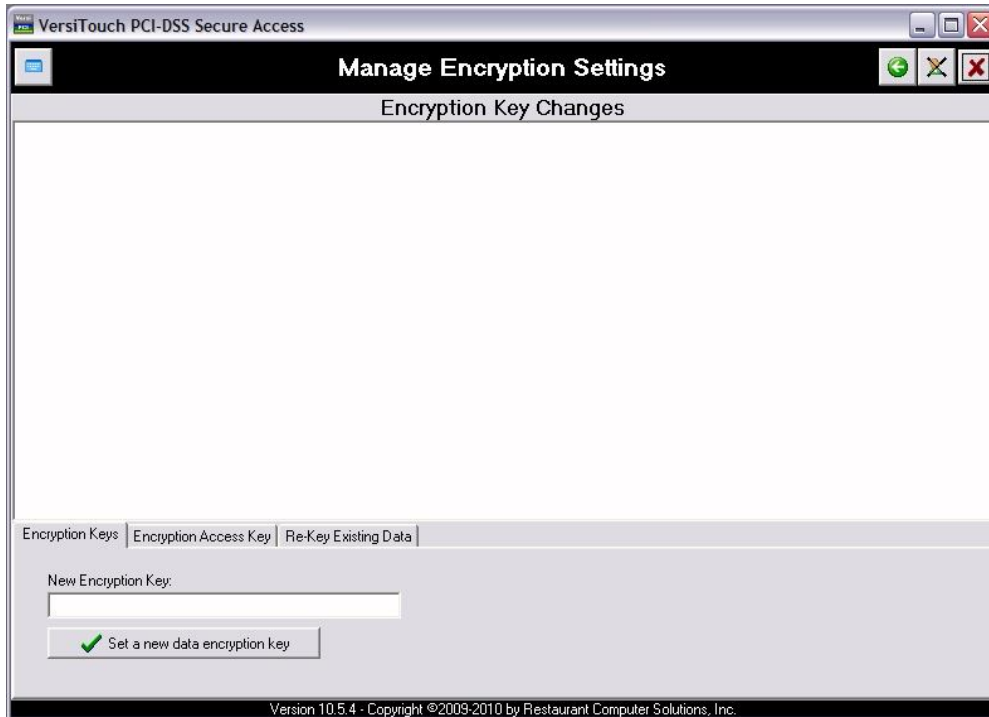
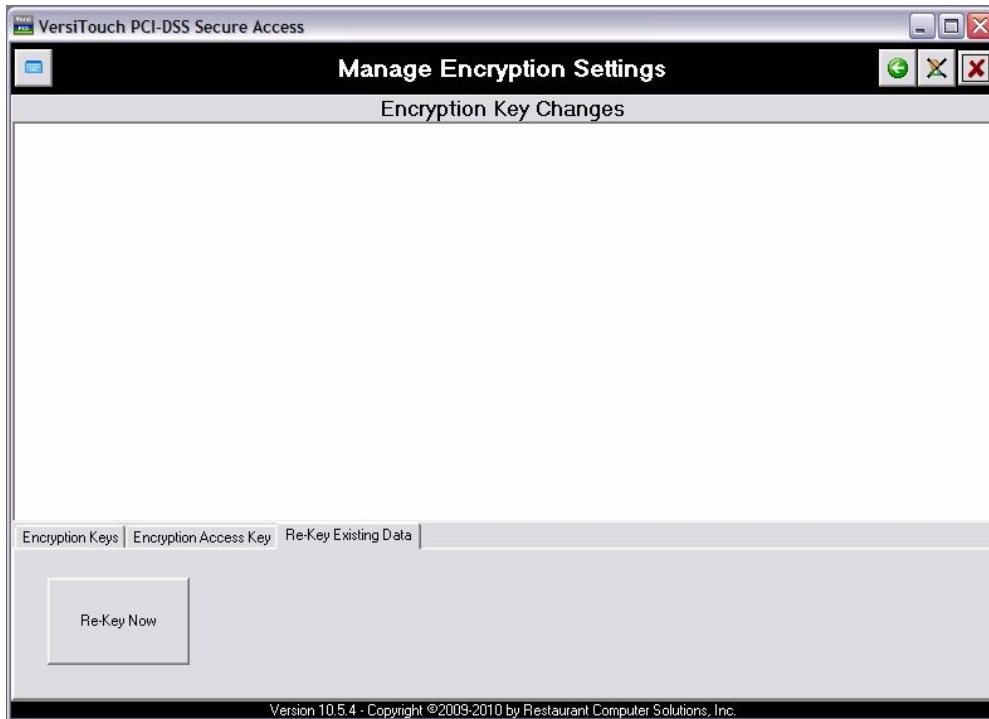


Figure 4-18. Manage Encryption Access Key



Figure 4-19. Re-Key Existing Data



# Troubleshooting

## 5

### FORCED BATCHES

Forced batches are credit card transactions that fail to transmit to the host processor at the time of settlement. This can happen for a variety of reasons ranging from communication problems (line noise, busy phone line, internet down, etc.) to cards being over limit at the time of settlement. When a batch fails to settle, the **VersiTouch POS** will typically give a merchant the option to force the batch. This allows the merchant to close the day's business, archiving the tickets and resetting all reports to zero (with a cash register, this same process is often referred to as "Z"-ing the system).

In rare circumstances, a problem may occur where the **VersiTouch Credit** software isn't detected by the **VersiTouch POS** software during the closeout. This can happen as a result of a network problem or something as simple as the PC that runs **VersiTouch Credit** being turned off. In addition to not being able to transmit the credit card batch, the **VersiTouch Credit** server won't be able to generate the files necessary for a forced batch. In a situation where the batch isn't settled but no force files are created, you can now use **VersiTouch Credit Access** to generate replacement force files. Refer to page 4-11 for instructions.

You'll note that the force files will be generated in the \RCS folder on the shared drive of the fileserver. This, however, may not be the location that your **VersiTouch Credit** software expects to find them. It may be necessary to manually move the force files to the folder that contains the **VersiTouch Credit** merchant configuration file (often referred to as the "RCM file" because of the .rcm extension).

After generating the new force batch file, follow the instructions for settling a forced batch found in the **VersiTouch Credit User Guide**.

### DELETING SENSITIVE CREDIT CARD DATA

In the process of deleting sensitive credit card data from daily closeout archives, the process can halt if the target data file is corrupted or invalid (most often, a zero bite file). Check the \RCS\STORAGE folder for any files of less than 1 kb and manually delete them; run the delete process, again.

# Glossary

## 6

### GLOSSARY

**Account:** See *'Merchant account'*.

**Acquirer:** An acquirer is a Visa/Master Card Affiliated bank or Bank/Processor alliance that is in the business of processing credit card transactions for businesses and is always acquiring new Merchants.

**Acquiring Bank:** A financial institution that provides credit card processing accounts for Merchants. Also referred to as a Merchant bank or an acquirer, the bank receives funds from a cardholder when a credit card transaction is completed, and then deposits the payment amount, less any fees, into the Merchant's business checking account.

**Authorization:** The process of verifying that a credit card has sufficient funds (credit) available to cover the amount of the transaction. An authorization is obtained for every sale. An approval response in the form of a code is sent to the Merchant's POS equipment. This process verifies that the card number and expiration are valid. In addition, it allows the bank to verify that the amount is within the customer's credit limit and to make sure the card is not stolen. See *also 'Voice Authorization'*.

**Authorization Response:** An issuing financial institution's electronic message

reply to an authorization request, which may include:

Approval -- transaction was approved  
Decline -- transaction was not approved  
Call Center -- response pending more information, Merchant must call the toll-free authorization phone number

**Authorization Code:** A code that a credit card issuing bank returns in an electronic message to the Merchant's POS equipment that indicates approval of the transaction. The code serves as proof of authorization.

### **Automated Clearing House (ACH)**

**File:** A file with instructions for the exchange and settlement of electronic payments passed between financial institutions. It represents debits and credits to be deducted from an account automatically as they occur.

**Bankcard:** A credit card issued by a Visa or MasterCard sponsored financial institution. (American Express, Discover, Diners Club, JCB, etc, are issued directly from their respective operations, rather than through banks.)

**Batch:** The accumulation of captured credit card transactions in the Merchant's terminal or POS awaiting settlement.

**Batch Close:** The process by which a Merchant gathers all of the credit card transactions that have occurred over a specified period of time, usually one full day, and submits them to the financial institution acting as the acquiring bank for settlement.

**Capture:** The submission of an electronic credit card transaction for financial settlement. Authorized credit card sales must be captured and settled in order for a Merchant to receive funds for those sales. Also see Settlement.

**Cardholder:** A person who holds a payment card account (bankcard or otherwise).

**Card Issuing Bank:** An EFT Network Member-Bank that runs a credit or debit card “purchasing service” for their account holders. An example is CitiBank and the CitiBank Visa Card that they issue.

**Card Not Present** A transaction where the card is not present at the time of the transaction (such as a mail or telephone order). Credit card data is manually entered into the terminal, as opposed to swiping a card’s magnetic stripe through the terminal. Also see Mail Order/Telephone Order (MOTO).

**Chargeback:** A credit card transaction that is billed back to the Merchant after the sale has been settled. Chargebacks are initiated by the card issuer on behalf of the cardholder.

**Close Batch:** The process of sending the batch for settlement.

**Code 10 Authorization:** If a credit card is suspected to be fraudulent at the time of the transaction, the Merchant can call their voice authorization phone number and ask for a code 10. The voice operator will instruct the Merchant on how to proceed.

**Corporate Cards/Commercial Cards:** Credit or charge cards issued to businesses to cover expenses such as travel and entertainment.

**Credit Card Software:** A POS Terminal Application or PC or Internet Application that runs transactions and associated administration.

**Credit (Reversal):** Nullification of an authorized transaction (sale) that has not been settled. If supported by the card issuer, a reversal will immediately “undo” an authorization and return it to the open-to-buy balance on a cardholder’s account. Some card issuers do not support reversals.

**Debit Card:** Payment card whose funds are withdrawn directly from the cardholder’s checking account at the time of sale (online debit on a Debit Network) or after batch settlement (off-line debit on a Credit Card Network).

**Electronic Data capture (EDC):** The process of electronically authorizing, capturing and settling a credit card transaction.

**EFT (Electronic Funds Transfer):** A method of transferring money from one bank account to another, using any of a wide variety of electronic methods currently available.

**Footer:** Text printed at the bottom of a sales draft. A Merchant can customize the footer (i.e., Come Again, Thank You, etc.).

**Force:** Refers to the method of manually processing a transaction or settlement. See also *'Voice authorization'* and *'Manual settlement'*.

**Force files:** These are the data files that are created when a settlement is forced. Force files contain the information that is required for the host processor to transfer funds to the Merchant's bank account. See also *'Manual settlement'*.

**Forced authorization:** See *'Voice authorization'*.

**Forced settlement:** See *'Manual settlement'*.

**Hardware:** The physical equipment that makes up a point-of-sale system. This includes computers, touch screens, printers, and any peripheral devices that are attached. See also *'Software'*.

**Host processor:** See *'Processor'*.

**Independent Sales Organization (ISO):** An ISO is an Independent Sales Organization that represents a bank or Bank/Processor alliance. The ISO has an agreement to sell the services of the bank or Bank/Processor alliance.

**Interchange:** The standardized electronic exchange of data associated with sale and credit data between Merchant Acquirers and Card Issuers.

**Internet Service Provider (ISP):** Internet Service Providers (ISPs) are the Web Site Hosting companies that provide a home for merchant's web sites. They typically resell and/or support the services of a Secure Gateway Provider and/or ISO or Agent or Bank.

**Issuing Financial Institution:** The Financial Institution that extends credit to cardholders through bankcard accounts. Also referred to as the cardholder's financial institution.

**Mag-card:** Any card that has data encoded on a magnetic strip. This usually refers to credit cards.

**Magnetic Stripe:** A strip of magnetic tape affixed to the back of credit cards containing identifying data, such as account number and cardholder name.

**Mail Order/Telephone Order (MOTO):** Credit card transactions initiated via mail, email, or telephone. Also see Card Not Present.

**Manual Close:** See *'Manual Settlement'*.

**Manual settlement:** Should the merchant's connection to the host processor be interrupted for an extended period of time, or there is some other problem with the settlement, a manual settlement can be used. This allows the POS to complete the closeout procedure normally, but does not actually send the settlement to the bank. Once this has been performed, the merchant must later use the **VersiTouch Credit** software to send the batch to the bank (after the problem has

been corrected). The advantage to using this feature is that it allows a merchant to continue on with the next day's business without having to immediately deal with whatever is causing the problem.

**Merchant:** The business owner or operator offering goods or services for credit card payment. A customer of a Processor/Acquirer.

**Merchant account:** The configuration that routes the funds received from credit card transactions to the Merchant's bank account. The merchant account is created by the credit card provider, as defined by the host processor.

**Merchant Identification Number (MID):** This number is generated by a Processor/Acquirer to identify an individual merchant and location during processing of credit card transactions.

**Merchant Services Provider:** A bank, ISO or any other firm that provides the various services required for the processing of a merchant's credit card sales.

**MSR:** Acronym for Magnetic-card Swipe Reader. The MSR is the physical hardware used to read credit cards. **VersiTouch Credit** requires a MSR that connects via a keyboard wedge interface and reads card tracks 1 and 2 of the mag-card.

**Network:** Two possible definitions:  
1. The software that is used to allow multiple computers to share information. **VersiTouch** products

operate over any network that allows mapping and sharing of hard drives.  
2. The primary processor protocol, such as VisaNet or Novus.

**PC Software:** A software program designed to perform a specific function on a computer system, such as a Restaurant Point of Sale System. The application must be interfaced with a credit card authorization system in order to provide on-line transaction processing.

**Point of Sale (POS):** The location where credit card transactions are performed with the cardholder present, such as a restaurant. The card is read magnetically, and the cardholder's signature is obtained as insurance against the transaction. This is the most secure form of credit card commerce.

**POS Terminal:** Equipment used to transmit and capture credit card transactions at the point of sale.

**Processor:** A Processor is the company that actually routes an Authorization Request from a Point of Sale device to Visa or MasterCard, and then arranges for Fund Settlement to the Merchant. Such processors can be accessed via direct dial out modems connected to their system, or via DSL.

Processors need to have a Sponsoring Bank in order to gain access to the Visa and MasterCard networks. When a Processor or other entity has made such an arrangement with a Sponsoring Bank to resell their services, they are called an Agent of that bank.

Any entity that sells Visa or MasterCard must disclose themselves as an Agent of their Sponsoring Bank. Such sales entities may be a Processor, or and ISO/Agent of the Processor or Processor/Bank alliance.

Many banks are also their own processors, while other banks will use a Third Party Processor to handle this processing for them (in their own brand name in some cases).

**Processing Network (Vendor):** The medium of data transport between the merchant application and the processor. This company authorizes and captures credit card transactions. **VersiCredit is certified for dial up processing with the processing networks Vital, First USA Paymentech, Novus (Discover), First Data Bank (Nashville Capture) and with Heartland Payment Systems and Mercury Payment Systems for broadband processing.**

**Provider:** The agent that sets up and manages your credit card service. This may be your bank or an independent agent. The provider works with one or more processors to offer credit card services to the merchant.

**Reseller:** A company that integrates hardware and software to provide a complete point-of-sale system.

**RCS:** Acronym for Restaurant Computer Solutions, the company that originally developed the **VersiTouch** family of POS products.

**Sales Draft (Ticket):** A form showing an obligation on the cardholder's part to pay money (i.e., the sales amount) to

the card issuer. This is the piece of paper that is signed when making the purchase. Sales draft data can be captured electronically and sent to be processed over the phone lines. Also see Electronic Data Capture.

**Secure Payment Gateway:** Secure Payment Gateway companies help other Processors conduct secure business on the internet using Secure Socket Layer (SSL) technology.

They provide a system that passes credit card data, authorization request, and authorization responses over the internet using encryption technology.

Rather than try and create their own Secure Web System, many Banks and Bank/Processor alliances will use a Secure Payment Gateway Provider to perform this task for them.

**Settlement:** The process of sending a Merchant's batch to the network for processing and payment. Every time the POS performs a shift/daily closeout, a settlement must be performed to capture the charges that have been authorized, post any credits that have been processed, and to void any canceled authorizations. Any authorizations that are not captured through settlement will be dropped and no money will be collected.

**Software:** The digital programs that control the input and output operations of a computer. Software generally refers to the programs (developed by VersiTouch) that allow you to enter orders at the POS station and to transmit credit card data to the processor. Your POS system also has

an Operating System and Network software that are not provided by VersiTouch.

**Split dial:** Processing credit cards through multiple processor networks depending on the card type that is swiped at the POS station. **VersiTouch Credit** does not support split dial or multiple merchant numbers.

**Station reset:** Turning the power at a POS station off and back on. This may be necessary if the station becomes unresponsive. *See also 'System reset'.*

**Swipe:** The action of moving a magnetic card (such as a credit card) through the MSR.

**Swipe Discount Rate:** The lower discount rate that is charged by an acquiring bank or Merchant Services Provider for transactions in which the credit card is present for inspection and read by a magnetic swipe reader.

**Sponsoring Bank:** A Sponsoring Bank is a Chartered Bank or S & L that has obtained membership in Visa or MasterCard in order to allow a Processor access to the Visa and MasterCard networks (in order to process these types of transactions).

Since only a Bank may join Visa or MasterCard, many Processors make deals with a Sponsoring Bank in order to gain access to the Visa and MasterCard networks.

Because these Sponsoring agreements are usually like a partnership, the line between the Sponsoring Banks and their Processors is not always clear;

sometimes the partnership is referred to by the name of the bank, while other times they are referred to by the name of the Processor.

**System reset:** Turning the power at all computers connected to the POS network (including stations and office PCs) off and back on. This may be necessary if the network software becomes unresponsive. *See also 'Station reset'.*

**T & E Cards:** Credit or charge card used by businesses for travel and entertainment expenses. Also see Corporate Cards.

**Terminal:** Equipment used to transmit and capture credit card transactions.

**Terminal Identification Number (TID):** This number is generated by a Processor/Acquirer to identify individual terminals within a Merchant's establishment during processing of credit card transactions. **VersiCredit uses only one point of connection, and therefore has only one TID.**

**Third Party Processor:** A Third Party Processor is an independent party contracted by a Bank or Processor to conduct some part of the credit transaction processing.

Some Third Party Processors specialize in the settlement of credit card transactions with Visa and MasterCard so that Merchants can be paid.

In the world of Internet Credit Card Processing, the Secure Payment Gateway Provider is another type of Third Party Processor. Rather than try

and create their own Secure Web System, many Banks and Bank/Processor alliances will use a Secure Payment Gateway Provider to perform this task for them.

**Transaction Fee:** A pre-determined and customary charge that is incurred for each individual credit card transaction a merchant processes, and collected by the Merchant Account Provider or the ISO.

**VAR:** Acronym for Value Added Reseller. *See also 'Reseller'.*

**VersiCredit:** The common name for **VersiTouch Credit**. **VersiTouch Credit** is the interface software that allows credit card transactions to be transmitted to the processor for authorization and settlement. *See also 'VersiTouch'.*

**VersiTouch:** The suite of point-of-sale software products developed by VersiTouch. The **VersiTouch** product family includes **VersiTouch POS**, **VersiTouch Office**, **VersiTouch Credit**, **VersiTouch Hotel**, and **VersiTouch Gift Card**.

**Voice authorization:** Occasionally, a charge is manually authorized over the telephone. In this case, the charge should not be authorized by **VersiTouch Credit**. The POS should record the sale as usual, recording the manual authorization number. On settlement, the charge is recorded as a FORCE in field #1 to indicate that the transaction was manually authorized.

**Void:** A void is the deletion of a previously authorized, but not posted,

charge. All voids are handled directly by the POS program. Any charges previously authorized that have since been voided should be, but are not required to be, included in the settlement file. Currently, most processors simply ignore voided authorizations. However, some processors do process voids and release the authorized amount from the customers credit limit, and others will probably support this feature in the future. If the void is not included in the settlement file, the charge will not be captured, and the authorization will eventually be released.

# Index



- Account. See Merchant Account
- Activating
  - VersiTouch Credit Access**, 3-2
  - Temporary Admin, 3-3
- Add Users, 4-6
- Delete PCI Data, 4-13
- Force, 3. See Manual Settlement. See Voice Authorization
- Force files, 3
- Forced authorization, 3
- Forced settlement, 3
- Generate Batch Force File, 4-11
- Glossary, 6-1
- Hardware, 3
- Host processor, 3. See Processor
- Installing
  - Where to? 2-3
  - License Key Drivers, 2-4
- Mag-card, 3
- Magnetic-card Swipe Reader. See MSR
- Manage Users, 4-4
- Manual settlement, 3
- Manage User, 4-7
- Merchant account, 4
- Modify User, 4-7
- MSR, 4
- Network, 4
- Provider, 5
- RCS, 5
- Remove User, 4-7
- Reseller, 5
- Restaurant Computer Solutions, 5
- Settlement, 5
- Software, 2-1
- Split dial, 6
- Station reset, 6
- Swipe, 6
- System reset, 6
- Troubleshooting, 5-1
- Value Added Reseller, 7. See Reseller
- VAR, 7. See Reseller
- VersiCredit, 7
- VersiTouch, 7
- VersiTouch Credit, 7
- VersiTouch Credit Access, 1
- VersiTouch Gift Card, 7
- VersiTouch Hotel, 7
- VersiTouch Office, 7
- VersiTouch POS, 7
- View Access Log, 4-8
- View Transactions, 4-9
- Voice authorization, 7
- Void, 7



**versitouch**  
www.versitouch.com **RCS**

V e r s i T o u c h , I n c .  
6019 SE 44<sup>th</sup> Avenue, Portland, OR 97206  
Voice (800) 655-7349, Fax (503) 788-5930

**VersiTouch Credit Access** is the only means by which a user can access full credit card information stored by the **VersiTouch Point-of-Sale** (POS) system. By limiting access to sensitive credit card data per the requirements of the PCI PA-DSS, we provide a payment application that makes it possible for you to achieve PCI compliance.

**VersiTouch Credit Access** requires activation by VersiTouch, Inc. Before we will activate the **VersiTouch Credit Access** utility for your location, we must verify the identity of the primary administrator. This can be achieved in one of two ways: 1. verification by a notary public; or, 2. verification by your installing reseller. After your identity is verified, mail this signed authorization form to VersiTouch, Inc. at the address listed, above.

Further, by signing this authorization form you:

1. Recognize and assume all risk that this utility could be used for unauthorized or unintended purposes, such as theft of sensitive credit card data from the merchant.
2. Bear all responsibility for controlling the use of this utility.
3. Agree that the utility will not be used for any illegal means or purposes.
4. Agree that the software license and 'key' that you received will only be used at the restaurant named below.
5. Agree that upon closure or change of ownership of the restaurant named below, the restaurant will surrender the license and 'key' back to VersiTouch, Inc...
6. Release VersiTouch, Inc. from any and all responsibility, monetary or other, of the intended or unintended use, results, side-effects, or any other issue related to this utility.
7. Agree that this license may be revoked at any time by VersiTouch, Inc. for any illegal or fraudulent use of the utility. If VersiTouch, Inc. revokes the license, the restaurant will surrender the license and 'key' to VersiTouch, Inc. within one (1) working day after notification of revocation.
8. Agree that the license to use this software may not be resold or transferred.

Merchant Name:	
DBA:	
Address:	
Phone:	
Owner/Officer & Title (printed):	
Signature:	Date Signed:

Before me, the undersigned authority, on this \_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_, \_\_\_\_\_ personally appeared to me well known to be the person who executed the foregoing instrument, and he/she acknowledged before me that he/she executed the same as his/her voluntary act and deed.

\_\_\_\_\_  
NOTARY PUBLIC

~OR~

*By signing this form, the VersiTouch reseller certifies that the owner/officer of the merchant identified above is a duly authorized representative of the Merchant and has voluntarily executed the foregoing instrument.*

VersiTouch Reseller:	
Reseller Contact:	
Signature:	Date Signed:



**versitouch**<sup>TM</sup>  
www.versitouch.com **RCS**

V e r s i T o u c h , I n c .  
6019 SE 44<sup>th</sup> Avenue, Portland, OR 97206  
Voice (800) 655-7349, Fax (503) 788-5930

## VersiTouch Credit Access

### Encryption Key Custodian Form

Per the requirements of the PCI PA-DSS, VersiTouch, Inc. provides a means by which the Data Encryption Key and the Key Encryption Key are separately managed within VersiTouch Credit Access.

Sharing this knowledge (whether between authorized users or other entities) reduces the effective security around sensitive credit card data stored by your VersiTouch Point of Sale system.

By signing this form, you acknowledge that you understand and accept your role as a custodian of the specified encryption key.

I, \_\_\_\_\_, as an assigned representative of \_\_\_\_\_ hereby acknowledge that I understand and accept my role as custodian of the (circle one):

Data Encryption Key

Key Encryption Key

\_\_\_\_\_  
Custodian Signature

\_\_\_\_\_  
Date



## END-USER LICENSE AGREEMENT

**IMPORTANT- READ CAREFULLY:** This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Restaurant Computer Solutions, Inc. ("VERSITOUCH") for the VERSITOUCH software product(s) accompanying this EULA, which include(s) computer software and may include "online" or electronic documentation, associated media, and printed materials ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT or any UPDATES (as defined below), you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install, copy, or otherwise use the SOFTWARE PRODUCT; you may, however, return it to your place of purchase for a full refund. In addition, by installing, copying, or otherwise using any updates or other components of the SOFTWARE PRODUCT that you receive separately as part of the SOFTWARE PRODUCT ("UPDATES"), you agree to be bound by any additional license terms that accompany such UPDATES. If you do not agree to the additional license terms that accompany such UPDATES, you may not install, copy, or otherwise use such UPDATES.

### SOFTWARE PRODUCT

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold, to you, and VERSITOUCH owns all copyright, trade secret, patent and other proprietary rights in the Software. NOTE: The terms of a printed, paper EULA which may accompany the SOFTWARE PRODUCT supersede the terms of any on-screen EULA found within the SOFTWARE PRODUCT.

#### 1. LICENSE TO USE SOFTWARE PRODUCT.

- A. Proof of License. A registered hardware key ("LICENSE KEY") is your proof of license to operate the SOFTWARE PRODUCT and must be physically installed on each computer where the SOFTWARE PRODUCT will operate.
- B. Registration of License. LICENSE KEYS are registered as a group to a single address or location ("SITE").
- C. General License Grant. VERSITOUCH grants to you, as an individual or single entity, a nonexclusive license to make and use copies of the SOFTWARE PRODUCT. You may install copies of the SOFTWARE PRODUCT on an unlimited number of computers provided that each of the computers has a registered LICENSE KEY.
- D. Documentation. This EULA grants you, as an individual or single entity, a nonexclusive license to make and use an unlimited number of copies of any documentation, provided that such copies shall not to be republished or distributed (either in hard copy or electronic form) beyond the SITE.
- E. Storage/Network Use. You may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT on computers in accordance with Section 1.C. A single license for the SOFTWARE PRODUCT may not be shared or used concurrently by other end users.

#### 2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

- A. Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT or LICENSE KEY.
- B. Derivative Works. You may not modify or prepare derivative works of the SOFTWARE PRODUCT.
- C. Rental. You may not distribute, sublicense, rent, lease, or lend the SOFTWARE PRODUCT or LICENSE KEY.
- D. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of VERSITOUCH.
- E. Software Transfer. The initial user of the SOFTWARE PRODUCT may make a one-time permanent transfer of this EULA, SOFTWARE PRODUCT, and LICENSE KEYS only directly to an individual or single entity. This transfer must include the entire SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, this EULA, and all SITE registered LICENSE KEYS). Such transfer may not be by way of consignment or any other indirect transfer. The transferee of such one-time transfer must agree to comply with the terms of this EULA, including the obligation not to further transfer this EULA and SOFTWARE PRODUCT. If you transfer the SOFTWARE PRODUCT and LICENSE KEY, you must erase any copies residing on computer equipment. Your license is automatically terminated if you transfer the SOFTWARE PRODUCT and LICENSE KEY.
- F. Separation of Components. The SOFTWARE PRODUCT and LICENSE KEY are licensed as a single product. Component parts of the SOFTWARE PRODUCT or LICENSE KEY may not be separated for use by more than one user.
- G. Termination. Without prejudice to any other rights, VERSITOUCH may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must return or destroy all LICENSE KEYS and copies of the SOFTWARE PRODUCT and all of its component parts.

3. **UPGRADES.** If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by VERSITOUCH as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this EULA.

4. **COPYRIGHT.** All title and intellectual property rights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, the LICENSE KEY, and any copies of the SOFTWARE PRODUCT are



owned by VERSITOUCH or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE PRODUCT is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. All rights not expressly granted are reserved by VERSITOUCH.

5. **EXPORT RESTRICTIONS.** You agree that you will not export or re-export the SOFTWARE PRODUCT, any part thereof, or any process or service that is the direct product of the SOFTWARE PRODUCT (the foregoing collectively referred to as the "Restricted Components"), to any country, person, entity or end user subject to U.S. export restrictions. You specifically agree not to export or re-export any of the Restricted Components (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, which currently include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria, or to any national of any such country, wherever located, who intends to transmit or transport the Restricted Components back to such country; or (ii) to any end-user who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government. You warrant and represent that neither the BXA nor any other U.S. federal agency has suspended, revoked, or denied your export privileges.
6. **MISCELLANEOUS.** This EULA is governed by the laws of the State of Oregon in the United States of America. Should you have any questions concerning this EULA, or if you desire to contact VERSITOUCH for any reason, please write to: VERSITOUCH, INC., 6019 SE 44<sup>th</sup> Avenue, Portland, OR 97206.
7. **LIMITED WARRANTY.** You expressly acknowledge and agree that use of the Software is at your sole risk. Except for the limited one (1) year warranty on the LICENSE KEY, the SOFTWARE PRODUCT and any related documentation or materials are provided "AS IS" and without warranty of any kind. VERSITOUCH EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. VERSITOUCH DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY YOU AND YOU (AND NOT VERSITOUCH) ASSUME THE ENTIRE COST OF ALL SERVICING, REPAIR AND/OR CORRECTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.
8. **LIMITATION OF LIABILITY.** UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE SHALL VERSITOUCH, OR ITS DIRECTORS, OFFICERS, EMPLOYEES, DEALERS, OR AGENTS, BE LIABLE TO YOU FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOST DATA, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT OF THE POSSESSION, USE, OR MALFUNCTION OF THE SOFTWARE, INCLUDING WITHOUT LIMITATION DAMAGE TO PROPERTY AND, TO THE EXTENT PERMITTED BY LAW, DAMAGES FOR PERSONAL INJURY, EVEN IF VERSITOUCH OR A VERSITOUCH AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS DEPENDING ON THE LAWS IN YOUR STATE. YOU AGREE THAT THE LIABILITY OF VERSITOUCH ARISING OUT OF ANY KIND OF LEGAL CLAIM (WHETHER IN CONTRACT, TORT, OR OTHERWISE) WILL NOT EXCEED THE AMOUNT YOU ORIGINALLY PAID FOR THE USE OF THE SOFTWARE.