ClientBase Windows Encryption Release Notes

ClientBase Version 3.04.00 New Features and Enhancements (released July 2008)

*****Upon saving or editing Credit Card numbers, ClientBase now validates the card number.** If the number is invalid, a prompt will occur "The credit card number entered appears to have a typographical error or it is not a valid credit card. Do you want to continue saving this record?" This prompt serves as a warning that there may have been a data entry error (typo).

Selecting YES saves the card As Is.

Selecting NO returns user to the card number field.

When editing an existing card number, validation does not occur unless the Card number field is modified. Validation occurs in Profile Cards Tab, Invoice Form of Payment Credit Card and CC Merchant, Invoice Booking Payment Credit Card and CC Merchant, Reservation Payment Due Date tab, Receipt Form of Payment CC Merchant FOP

**Note regarding validation process:

valid credit card numbers with spaces do not prompt

valid credit card numbers with letters (VI1234123412341234) do not prompt

valid credit card numbers with expiration date after a slash (CA5458004519231383 /1109) will not prompt (although we do not recommend entering the expiration date in the Card Number field.)

*****Upon installation of both CBP 3.4 and TBO 3.01, Credit Numbers become encrypted and masked within the database.** In an effort to protect your clients from credit card fraud, and to comply with recent PCI (Payment Card Industry) Compliance regulations, all credit card numbers within your database have been encrypted and masked. To a typical ClientBase User this encryption appears invisible, but it makes the extraction of this personal data much more difficult should your database be accessed in an unauthorized manner. Upon retrieving a Credit Number within the ClientBase application, the system will automatically decrypt the credit card number and display the full number as always. (Please note the User Permission enhancement below where Users can be forced to only view the masked version of the Credit Card number.)

Introduction

The payment card industry (PCI) compliance and validation regulations spells out what security measures must be taken to protect the private information during any transaction occurring with the use of a paycard. The PCI Data Security Standard is used by all card brands to assure the security of the data gathered when transacting on behalf of a customer.

There are numerous regulations including encrypting the credit card numbers in the database. Encrypting this data makes it virtually impossible to decipher a credit card number without a decryption key which protects the credit card information in your database from fraudulent abuse.

How it Works

After running the cbplusup.exe the credit card data that was stored in the Credit Card field pre-encryption now contains a masked version of the credit card number. A new field is also added to the database. The full credit card number is copied from the existing field to the new field and then encrypted.

A cleaning and masking routine will take place during the database update to standardize all of the credit card numbers so they can be properly masked for all applications utilizing the masked Credit Card field. Only valid credit card numbers will be cleaned and appear in the masked format.

The valid credit cards will be standardized using these rules:

Any non-numeric text at the beginning of the string up to the first digit is stripped out. AX 3782 078 234 0834/1008 becomes 3782 078 234 0834/1008.

All spaces are removed. 3782 078 234 0834/1008 becomes 37820782340834/1008.

The credit card string is truncated starting at the first non-numeric character, usually a slash, leaving only digits. 37820782340834/1008 becomes 37820782340834 .

The format used for masking is:

2 letter card code + space + first 2 digits+ '-XXXX-' + last 4 digits (i.e. MC 54-XXXX-2364).

Three fields in the database relating to the credit card number:

Masked CC Number Field (CCNUMBER): Credit card number in masked format. Credit card numbers are standardized and validated. Valid credit cards are saved in its masked format and invalid credit cards are saved as is.

Encrypted CC Number Field (NUMBERENCRYPT): Encrypted full credit card number entry (all numbers whether valid or not are encrypted).

Hash CC Number Field (NUMBERHASH): Credit card number in hash format. This field is used for "faster searching of credit card number". Valid credit cards hash the standardized format. Invalid credit cards hash the number as is.

Status of ClientBase Utilities:

Utilities Updated: Globalware Invoice Export Utility, IC Host Utility, XML Travel History Import, Australian "Enable Automatic XML Profile Export",

Utilities Sunset (will no longer work after a database has been encrypted): XML Import, XML Export, CB2CBP conversion utility, CBT2CBP conversion utility

Utilities Not Affected: ASCII Profile Import, IB Backup, Ensemble Import, Ensemble Export, Virtuoso Utility, Virtuoso Segment Update

Use of Encryption Keys for Third Party or Custom Development:

A unique key will be generated for each agency that can be used in product development for non-TRAMS applications that need to read the full credit card number. The key can be obtained by the SYSDBA User only by going to Utilities|Credit Card Encryption Key and entering a password provided by the TRAMS support desk. A CCEncrypt.dll file is installed that allows access to the TRAMS database to view un-encrypted credit card numbers. Documentation for use is available upon request by e-mailing Customercare@trams.com. The intended audience is for the designers and developers of non-TRAMS applications that read credit card numbers directly from the TRAMS database.

*****Enhanced the User Login Advanced permission settings|Other Permissions to include the ability to "Mask Credit Card Numbers".** This allows you to mask full credit card numbers from Users that don't have a need to view the complete number. ClientBase Plus version 3.04 and TRAMS Back Office version 3.01 both must be installed and the database must be encrypted for this setting to be activated. All existing Users default this setting to unchecked. Upon checking this Advanced permission and saving, the system prompts with a message: "By checking Mask Credit Card Numbers for this User, Credit entries will not be included in Merge to PNR and Live Connect, since the full Credit

Number must result at the end of these features." Please keep this limitation in mind when deciding which Users should have the Credit Card numbers masked.

The following areas are updated if the current User Login is set to "Mask Credit Card Numbers":

Profile|Cards grid and Credit Card records mask the Credit Card Number and set to read only (in addition to Card Type)

Family Member|Cards grid and Credit Card records mask the Credit Card number and set to read only (in addition to Card Type)

Merge to PNR Selection Screen no longer includes any Credit Card data to select from

Live Connect Selection Screen no longer includes any Credit Card data to select from

Res Card Reservation Deposit FOP does not show the drop down list of CCs although a CC number can be hand entered. Upon saving the number will be masked.

Existing Res Card Reservations with a CC number, displays as masked although it can be edited and saved

Generate - Invoice feature does not include the drop down list of CCs although a CC number can be hand entered

*****Updated the Help/About screen to identify the status of credit card encryption.** "Credit Card Encryption Done" is either set to True or False depending on the status. In order for Credit Card Encryption to occur the database must be upgraded to ClientBase version 3.4 and TRAMS Back Office version 3.1.

*****Added a prompt when doing a Live Connect to a provider's website that doesn't use HTTPS.** This message warns about the lack of HTTPS and asks the user if they want to cancel, send all the information except the login/credit card or send all information including login/credit card.

*****File | Export | Profile Cards Info now exports the Credit Card Numbers as masked by default.**

*****Renamed the field within the database for Credit Card "NUMBER" to "CCNUMBER".** This was done to accommodate the Oracle version of our database, as Oracle does not allow a field name within the database called NUMBER

ClientBase Version 3.04.01 to 3.04.04 Fixes

- Fixed an issue in the CBPlusup.exe that resulted in an error when encrypting a database on Interbase 6. Users that have already encrypted the database do not need to run this update.

- Addressed issue where cbplusup.exe was not assigning permissions for dbencrypt procedure to SYNCUSER - caused invoices with no bookings to sync to the primary database.

ClientBase Version 3.05.00 New Features and Enhancements (released May 2009)

No new Enhancements or Features related to encryption

ClientBase Version 3.05.00 to 3.05.02 Fixes

- Fixed an issue with encrypted databases where users that were not restricted from seeing the full credit card number were not able to select a card number when issuing a receipt with form of payment CC Merchant.

- Addressed an issue where the encryption process was not correctly masking any credit card numbers with dashes (i.e. 4111-1111-1111-1111). When running the cbplusup.exe, any credit card numbers with dashes will be correctly masked.

ClientBase Version 3.06.00 New Features and Enhancements

*****Enhanced Credit Card masking permissions for further PCI Compliance.** Renamed the User Permission setting under Other Restrictions “Mask Credit Card Numbers” to read "Disable ability to view full Credit Card Numbers"

When this setting is checked the program will prompt with message "By checking "Disable ability to view full Credit Card Numbers" for this User, Credit entries will not be included in Merge to PNR and Live Connect, since the full Credit Number must result at the end of these features."

Also, when this setting is checked, only the masked version of the credit card number is shown in the following locations in the system:

• Profiles - Cards Tab
• Res Card - Reservations|Payment Due Date Tab
• Invoicing Screen - Invoice Payment Section
• Merge to PNR Selection Screen
• Merge to PNR Preview Screen
• Live Connect Screen

When Disable ability to view full Credit Card Numbers is unchecked, a masked version of the credit card number is shown in all areas above with the following exceptions:

• Profile - Cards Tab: Clicking Modify will show the masked credit card number with a button “View Full Number.” When this button is clicked to view the full credit card number user is prompted, "Do you really need to see the full credit card number? To keep customer data safe you should minimize the number of times sensitive data is visible. Keep in mind that your access will be logged.” Click Yes to continue and view the full number. This will also create an Edit Log documenting the User who viewed the number, the Date and Time the number was viewed and a Description (noting that credit card number was viewed). Click No to remain on the screen with the masked version.

• Merge to PNR data sent (whether clipboard or API) will send the full credit card number

• Live Connect data sent will send the full credit card number

*****Added "Mask Credit Card Number" feature to Utilities for removing credit card information for Payments, Booking CommTrack CC Numbers and Reservation Deposit CC Numbers that may no longer be of use.** To use this feature the database must be credit card encrypted. Masking the credit card number removes the full encrypted credit card number and replaces it with a masked version of the number.

Select Utilities|Mask Credit Card Number. In the Records to Mask field, choose the type of record to remove from the drop down. ClientBase only database options for removal are Payments, Booking CommTrack CC Numbers and Reservation Deposit CC Numbers. ClientBase databases that are Trams Back Office also, can only remove Reservation Deposit CC Numbers. Payments and Booking CommTrack CC Numbers affect accounting data and therefore removal must occur in the TBO program.

In the “Purge As Of” field, enter the Purge Date. For example, if you wanted to remove records prior to 01/01/2008, the Purge Date is 12/31/2007. Records are removed by date as follows:

- Payments (by Payment Date)
- Booking CommTrack CC Numbers (by Depart Date)
- Reservation Deposit CC Numbers (by Deposit Due Date)

After entering the purge date click the “Mask” button. A message appears indicating what type of records will be masked and as of what date. Click Yes to continue or No to return to the selection criteria.

ClientBase Version 3.05.05 to 3.06.00 Fixes

- Addressed an issue where credit card numbers were not masked when selecting a new credit card on the Reservation Payment Due Date tab. The database update (cbplusup.exe) will re-run the encryption routine to re-mask any valid credit card numbers.