Data security breaches represent a costly threat to any business.

Customers want more assurances and understandably, so do you.

The Epicor Eagle Transactional Security solution is designed to address this situation head-on and can provide freedom from worry about stolen bankcard data.

This service can remove all credit card numbers from Eagle and can ease the PCI certification process.

Your POS and transaction-related functions within the Eagle system work exactly as they did before and it is available for all of the major bank card brands.

We will review the system requirements for using this function, explain exactly how it works, discuss a useful utility to convert any stored credit card numbers and go over the needed device set up.

To use this feature you must be on Eagle N Series Release 24.1 or higher and it is only available to Epicor Payment Gateway customers.

You must be processing payment cards on the Epicor Gateway with one of the following processors.

FDMS

Global

Chase Paymentech

EPX

or RBS Worldpay

RBS Worldpay will be available in March of 2016.

After purchasing Transactional Security, Eagle Licensing will contact you to activate Option ID 1345, ‘Point to Point Encryption on System’.

Your credit card signature capture units will need to be Ingenico brand, model ISC 250 pin pads or newer.

Level 12.01 or higher RBA firmware will need to be downloaded on these devices.

If you have any questions about these requirements, you can easily check with your Epicor Customer Account Manager by calling this number.

Let’s discuss ‘Point-to-point Encryption’.

When your consumer swipes or inserts their bankcard, the actual bankcard number is immediately encrypted all the way to the Epicor Payment Gateway.

There it is unencrypted and then re-encypted to send along to the correct processors.

With ‘Point to Point Encryption’, no actual bankcard numbers will be stored, transmitted or processed by your Eagle system or your network.

Next we will explore the idea of ‘Tokenization’.

Instead of using a bankcard number, the Eagle system acquires a ‘token’ from the Epicor Payment Gateway.

This token represents the card number but is created by replacing the middle portion of the card number with other characters.

The result is specific to the card, to your retail business, and to your Eagle system.

Even if theft allows a third party to acquire a transaction or house account file, they won’t find a card number they can reuse.

However, you can still reuse a token, should you need to process a credit or a return.

Each token retains the first 6 digits and the last 4 digits of the credit card number.

This allows your staff and your customer to recognize the card.

If the store manager needs to authorize a credit on a purchase, he or she can use the token stored in Quick Recall to issue it back to the original credit card.

Before you implement Transactional Security, you have a choice to make regarding old bankcard numbers that are stored in Quick Recall. These card numbers will not be tokenized or encrypted.

You can leave them as is and as you run Transactional Security they will be removed per Option 311 “Days to store credit card numbers in Quick Recall”

These numbers can still be used to process credits and refunds but you will still have full bankcard numbers viewable from your system.

A second option is to truncate all the bankcard numbers in Quick Recall.

You will not be able to use these truncated numbers for credits or refunds.

Run this process before you turn on Transactional Security.

In the Eagle Browser under ‘Utilities’ [pause], click ‘Osprey’, [pause] and then log in as you normally would.

Type in the letters, ‘QRCCC’ and press Enter.

Choose ‘A’ to ‘Truncate all’

Then enter an ‘E’ next to ‘Action’ to Execute the process.

Press ‘ENTER’.

A screen will display with a summary of the records truncated in Quick Recall.

Press Enter to Continue and then type ‘Exit’ to close Osprey.

Now you can begin loading version 12.01 or higher on your pin pads.

Reboot the signature capture pad and verify that it is plugged into the PC. Make sure it is powered on.

Now, open ‘Device Configuration’ under the ‘Utilities’ menu in your Eagle Browser.

Double Click ‘Credit/Debit Pad’ from the main menu. [pause]

Then, note the current port setting, here. [pause]

Now press the ‘Device’ button. [pause]

Select ‘Ingenico isc250, RBA 12.01’ or the highest value displayed.

Depending on your system, you may see 14.04 or 15.05 listed.

Choose the highest value available and click ‘OK’.

Now press the ‘Download’ button.

This process can take 10 to 45 minutes depending on what version of RBA you were on previously.

After the download has completed, the PIN pad will briefly process the download file and then reboot.

Double click the ‘Credit/Debit Pad’ line and confirm that the Port listed matches what was noted earlier.

To change it, click ‘Port’ and scroll to the correct value.

In our example it was COM1.

Press ‘OK’.

Now choose ‘Options’.

Mark the check box next to ‘Transactional Security (P2PE)’.

Press ‘OK’.

You are now ready to test the pin pad.

Testing instructions can be found by pressing the button labeled ‘Docs’ from the ‘Credit/Debit Pad’ dialog box.

If you currently have stored credit card numbers for you AR customers you can run a utility to convert them to tokens. Simply display a customer record and open the ‘Go To’ Menu.

Select ‘Credit Card’ under the ‘Maintain’ section.

From the Credit Card Maintenance window choose ‘Action’ [pause] and then select ‘Convert Stored Cards to Tokens’.

Choose ‘Yes’ from the dialog box that appears and the credit card data for all stored credit cards in MCR will begin to convert to tokens.

When the process is complete, the following window will identify the number of records that were converted.

When the credit card maintenance window is displayed, you will now see the token instead of the actual credit card number.

Do not run the process to convert stored cards again or any other PCI Compliance function going forward with tokenization now in place.

If you would like to remove all bankcard numbers from Eagle you will need to purge the Protobase files.

This will require creating a Service Request with the Eagle Advice Line. They will be able to assist.

Transactional Security service will reduce time and effort required for the PCI certification process.

Your customers can confidently store their tokenized credit card numbers and authorize payment for deliveries, special orders or to pay off existing invoices.

By verifying some basic system requirements you could be on your way to providing a safe, secure and efficient bankcard environment for your customers.