Tech Tip Tuesday— February 10, 2015

by David Hirsch

Credit Card Encryption

As you know from the news, the issue of credit card encryption and databases "getting hacked" has been a popular topic lately.

There are rules in place by the Payment Card Industry (PCI) to try to limit the risk of someone stealing credit card numbers from databases—when the rules are followed, you are "PCI Compliant".

While total PCI compliance for your organization also involves your IT professionals (since it includes requirements on Windows passwords, firewalls, etc.) one important way that Livery Coach enables PCI Compliance is by completely encrypting all credit card numbers in your database.

We also limit the viewing of the full credit card number by restricting the viewing only to those agents with explicit permission, and logging each time the full credit card number is viewed.

One extremely important aspect of encrypting the credit cards in your database is that, even if someone were to get his or her hands on a backup of your database, and restore it somewhere else, the credit card numbers would still be unreadable—because the encryption key is stored elsewhere in the system.

This is all well and good, and has to be this way for security purposes.

HOWEVER, what this also means is that if you decide to upgrade your SQL Server or otherwise decide to move your data, you MUST contact Livery Coach tech support well in advance of such a move.

We do have special tools to be able to separately extract your encryption key from your database, and tools to enable us to apply this key to your database in the new location. But we need to know in advance of any move, so we can schedule the extract and encryption procedures.

As we have upgraded each of you to the credit card encryption version of Livery Coach, we have in most cases stored a password-protected copy of the exported key on your SQL server in the C:\Livery directory, and in many cases we have also kept a backup of this key on our system, just in case.

The existence of the key file is not sufficient to enable credit card decryption/encryption on a new SQL server (the password and tool are also needed), but without the key file the password and tool are not enough.

We are currently in the process of auditing our records to see if there are any keys that we are missing—and if so, we will contact you so we can make sure we both have a copy. But in the meantime, do not plan on any server moves or changes without consulting us first.