Dear Partners,

Our Connected Payments solution is best in class in the industry! It provides the most secure options for integrated payment processing available today. Over the years, we have tried to keep our Partners and Customers informed on PCI requirements and the continual changes that move PCI certification.

Last year and early this year we had numerous discussions around hardware point-to-point encryption ("P2Pe") and software encryption. Both solutions not only offer a secure, PCI compliant option, but it appeared that they would both lead to a de-scoping of POS. With the latest 3.1 version of the PCI requirements however, it appears that only the hardware P2Pe will have a path towards a de-scoping solution. The only way to have the POS out of scope requires a SRED (Secure Read and Exchange of Data) device and we then have to complete a detailed audit with each manufacturer. We are well into the audit with Equinox (L5200 and L5300), and we are just beginning the audit with VeriFone (MX920 and MX925) as well Ingenico (iSC250 and iSC350) devices.

Older PIN pads that are not SRED compliant — such as the VeriFone MX8xx devices and the older Hypercom 42xx devices — can still support the new hardware P2Pe using Connected Payments OpenEPS version 828.1 and the proper device upgrades. This solution will provide the most secure option available, short only of having the POS de-scoped using SRED devices. One other critical point is that to enable P2Pe, the proper Connected Payments hardware encryption key must be present in the PIN pads. If you are buying PIN pads from a source other than Retalix, you must ensure that the Retalix hardware encryption key is injected for the device to support P2Pe.

While this direction for P2Pe provides the ultimate security and/or putting the store and enterprise out of PCI scope, remember this does ***not*** mean that software encryption options are in any way non-compliant! Here are a few key facts that are important to understand as it relates to software encryption.

- In devices such as the MX8xx using software , the card data has a minimal level of encryption applied from the PIN pad. We use extremely secure AES128 to encrypt Track 2 data, but some Track 1 characters will be in the clear within the terminal hardware's memory. Of the data being decrypted, only the 16-digit number is decrypted into memory. Critically though, the Track 2 data is not, so there is no useful data for anyone to scrape from terminal memory.

- This is perfectly acceptable to PCI so long as the data is not stored — such as written to a file/placed on the hard drive — which in our case it is not. No PCI sensitive data is ever passed to our POS applications or stored. Card numbers arrive with the middle digits

erased, and the remaining digits are stored in the T-Log with zeros filling the gaps. PCI explicitly excludes any such "truncated" card numbers from their definition of "card data" or "customer data."

- Network security is the first line of defense, and helps prevent would-be hackers from being able to memory scrape this data as well. This is another factor in PCI compliance that should not be overlooked. Secure networks will prevent unauthorized out-going data just as carefully as unauthorized in-coming data.

- The PIN pads are critical: we may be limited in how much security we can provide depending on the PIN pads used. Some older models send the data in the clear before we can encrypt it. Some new models may offer some basic encryption, but we then must re-encrypt to provide a more appropriate level of security. While legacy devices can be made more secure by implementing hardware P2Pe, the best option is to invest in new SRED devices plus hardware P2Pe. Customers with legacy devices that cannot support hardware P2Pe should invest in new devices as soon as possible: this will not only increase their security and reduce risk, but is the only path toward taking their stores and enterprise out of PCI scope.

We understand: there is a lot of FUD out in the market related to payment systems, making it especially important to understand the facts and help keep your customers at ease. Be assured that Connected Payments continues to be PCI compliant and listed on the PCI website. Please let us know if you have additional questions.

Thanks,

Derrick

Derrick Hurley
Vice President
Retail Channel Sales, North America
derrick.hurley@ncr.com