Update Bulletin

New PCI Rules Affecting Dealers and Users

November 4, 2010

The PCI Council has just released version 2.0 of the PCI Data Security Standards (DSS). These new standards go into effect January 1, 2011, when all audits and self-certifications must be performed using the DSS 2.0 standards.

Among the many PCI DSS 2.0 differences, at least two are major changes that directly affect POS dealers and transform how dealers must manage their installed base and customers.

Each of these two changes, plus recommended and required actions affecting dealers and analysis for your users, is provided in this Update.

CHANGE: DATA PROTECTION RESPONSIBILITY

A "Service Provider" — which PCI defines as any third party that has access to unencrypted card data — must now accept responsibility for protection of that data, and every such Service Provider is required to pass a PCI Service Provider audit.

The PCI DSS 2.0 requires retailers to maintain a formal written agreement with each one of their Service Providers acknowledging that responsibility. This will dramatically affect dealers, since PCI now apparently regards dealers as Service Providers. The list of Service Providers includes:

- ***Processors*** — nothing new here, since Processors have always obviously handled unencrypted card data and have been required to maintain PCI compliance at the Service Provider level.
- ***Connected Payments*** — nothing new here either. Connected Payments transmits and stores all card data in encrypted form, but the Connected Payments system has the capability to decrypt data. The Connected Payments data centers are therefore required to be regularly audited and maintain Service Provider PCI. (A new version of the Connected Payments agreement is now available on the StoreNext Dealer Support Web site that includes the necessary responsibility and protection language.)
- ***Internet Service Providers ("ISPs")*** — this ***is*** new. If data from a store is sent to the processor "in the clear" — unencrypted — then the ISP is considered a Service Provider under PCI DSS 2.0 and must be audited and maintain PCI compliance, and the store must have an agreement in writing with the ISP acknowledging the ISP's taking responsibility for the security of that data.
- ***Wholesaler and Third-Party Networks, Leased Lines etc.*** — for the same reason as an ISP, any network carrying unencrypted data as part of the path to the processor must achieve PCI Compliance and the user must have an agreement with the wholesaler or network acknowledging that carrier's responsibility for the security and protection of that data.
- ***Dealers!*** — It's hard to believe, but DSS 2.0 interprets dealers — except for Connected Payments stores where all cardholder data is encrypted — as Service Providers. The reason is that old interfaces, such as Concord or EFT Manager, ScanMaster V1 EPI, and even WinEPS, permit dealer access to unencrypted card data during storage or transmission. So, according to PCI — and just like with any other Service Provider:

- Each of the dealer's end users must have a signed agreement with the dealer acknowledging the dealer's responsibility for security of the user's data
- The dealer must be audited for, and achieve, PCI Compliance
- This requirement was published by PCI for self-certifying retailers within the Self-Assessment Questionnaire (SAQ) as well as merchants being audited by a QSA.

According to the DSS 2.0, this means that any customer with unencrypted data would fail PCI Compliance unless the dealer has achieved PCI as a service provider.

Unfortunately, achieving PCI Compliance will place a major financial and operational burden on dealers, imposing extensive controls, new procedures and record-keeping on the dealer's staff, restricting and controlling access to software, changing how POS software, payments software and hardware is managed, installed and maintained, restricting or eliminating remote access and so forth. It appears that bonding will likely be required of all employees with access to software or the customer sites, and users may require dealers to carry additional insurance.

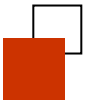
CHANGE: MANUAL ENTRY

Card numbers that are manually entered (where the PIN pad can't read the mag-stripe and the card number is entered on a keypad) are now fully considered to be "card data." In the past, manually entered card numbers did not have the same degree of scrutiny.

- Connected Payments and up-level WinEPS enable manual entry to be carried out at the PIN pad, where security protections such as encryption are in force.
- Dealers should make sure that the "manual entry" parameters in ISS45 and ScanMaster are turned off so that manual entry from the POS application is disabled.
- Performing manual entry on the PIN pad also re-establishes POS "isolation" from PCI data according to the new DSS 2.0 definition for manually entered card data. Again, Manual Entry in the POS application is perfectly legal, but would now bring POS into PCI scope under the new rules.

RECOMMENDED AND REQUIRED ACTIONS

1. Migrating your base to Connected Payments will make the whole issue go away. Connected Payments provides PIN-Pad-to-Processor encryption, which removes any possible dealer access to unencrypted data. This will exempt the dealer from PCI.
2. Change the manual card number entry parameters in all POS systems to enforce entry at the PIN pad only. This will handle manual card data within the payments system where it is already properly secured, and close this loophole where a dealer could "see" card data and be considered a Service Provider and liable for PCI.
3. If you can't migrate your base to Connected Payments, start working now on your PCI Service Provider Compliance. Of course, a QSA may choose to ignore or re-interpret the text of the DSS, and it's always possible that the PCI Council could retract, delay or rewrite the requirement in the future so that dealer access to unencrypted data wouldn't matter. But unless a dealer is willing to bank on that, the first customer requiring dealer PCI Compliance, just to pass their own PCI, will create critical problems for the dealer.
4. When being audited or self-certifying for PCI, your Connected Payments customers will be required to update their StoreNext agreement. The new version of this agreement meets the new PCI Service Provider requirements by adding a new section where StoreNext acknowledges responsibility for the protection of cardholder data while that data is in StoreNext's control.
    a. The new version of the agreement is available by clicking here or from the Connected Payments All-In-One Page on the StoreNext Dealer Support Web site.



b. This is a new agreement and therefore a re-start with new anniversary dates. But whatever pricing or program was in place from the original agreement will be treated as if the original agreements were in force. No down-sides to pricing.
c. Customers will want to take advantage of the new agreement anyway, since this version provides the benefits of better termination terms, the service level warranty and the protection of Customer Data. All or some of these terms were not included in various earlier versions that your customers may have signed.
d. Only the main body of the agreement needs to be signed and forwarded – there will be no need to resubmit the exhibits.

These issues will be discussed by the MTXEPS presenters at the Electronic Payments Industry Update sessions at the Synergy User Conference starting on Tuesday November 9 at 11:15 a.m.

To get the latest PCI documentation, including the new PCI DSS 2.0 and the new PCI DSS Self-Assessment Questionnaire (SAQ): click here.

ANALYSIS

Retailers need to understand that:

- With these ever-more stringent PCI requirements, it is clear that the card associations are forcing all hands throughout the payments industry to adopt solutions that provide encryption to lower the risk of data losses.
- Although it is still ***technically*** possible to achieve PCI Compliance without encryption, the compliance requirements around other methods have been made either too expensive or impractical. Now, PCI DSS 2.0 requires the entire chain of Service Providers to achieve Compliance themselves — plus sign up to take responsibility for the protection of cardholder data. This makes the cost unsupportable for transmission or storage of data "in the clear" starting with the dealer and going all the way up the chain.
- Although PCI stopped short of mandating encryption as the ***only*** solution, this step appears inevitable.
- This all adds up to the days being over for the previous generation of technology and methods. Like it or not, the age of in-store payment applications and in-the-clear transmission has passed; retailers have no practical choice but to migrate to new methods.
- Connected Payments fortunately provides the industry's single best solution, offering PIN-Pad-to-Processor encryption with full and tight POS integration, plus isolating the POS from card data. You have the only solution in the business that can do this.
- Dealers are already experiencing competition from "encryption-only solutions" that muddy the water with your customers. These are often proposed directly by the processor without your knowledge. But these products do not integrate with the POS, and are suited only as stand-beside PIN pads, missing most of the features grocers need and already take for granted.
- Responding to these situations puts the dealer on the defensive, trying to explain complex integrations, BIN files, etc. to customers who have been confused by third-party promises that cannot be implemented. You don't want to get called in to support an impossible request to make third-party encryption work after the deal is already done, so it's critical for dealers to get to the customer ***first*** with a Connected Payments proposition that protects both the customer and the dealer.

To Your Success,

Antony van Seventer