

What you should know about credit cards and PCI compliance

By Ed Becker, ADP Product Marketing

Credit cards are a fact of life for all dealerships. This memo is designed to help orient you as you embrace your responsibilities with regard to the Payment Card Industry Data Security Standard (PCI DSS).

This memo does not provide detailed recommendations or actions you may need to take to achieve compliance.

Visa, MasterCard, Discover Card, American Express and the Japan Central Bank developed the Payment Card Industry (PCI) Data Security Standard (DSS) in 2004. This global standard is designed to guide all organizations accepting credit cards to secure their operations and therefore minimize the chances for fraud. It does so by defining controls (both process and technology controls) for handling cardholder data that minimize the risks for all involved.

PCI compliance is the responsibility of all merchants accepting credit cards issued by the PCI-associated card brands. Even if you only accept one card annually and simply use an imprint device, you must meet certain PCI Data Security Standards. Specifically, the PCI standards state that if you *process, store, or transmit* credit card information you must meet the PCI Data Security Standards.

Reports of merchants who ignored the standards and experienced a breach indicate that fines imposed on such merchants may be more severe than for those who made efforts to comply and experienced a breach. ADP recommends that you read at least a few of the breach cases available on the Internet by executing a simple search on 'credit card breaches' to become familiar with the implications of a breach. The Ponemon Institute estimated that the average cost of a breach is currently around \$7.2 million. (<http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher>)

Specifically, if you are a merchant who accepts credit cards for payment, you are responsible for the following:

- Reviewing and understanding the PCI Data Security Standards*
- Understanding the reporting requirements that apply to your business
- Reporting compliance to your payment processor annually

Most dealerships fit into the small-to-medium business classification with respect to credit card processing and will be defined as level 3 or 4 merchants. The good news is that these merchants, while still expected to comply with the PCI DSS, may have simpler reporting requirements in the form of self- assessments.

ADP has worked with PCI-compliant payment processors to bring 3rd-party solutions to market. These solutions prevent credit card information from being processed, stored or transmitted on your DMS. The solutions employ:

- Encryption of the card data when it is swiped or entered
- A PCI PTS* validated tamper-proof card reader

ADP analysis of the PCI DSS leads us to the understanding that delivering PCI DSS-compliant solutions on a DMS network can be very complex and costly. Therefore, ADP has a policy in place to not build and sell credit card point-of-sale products.

Instead, our policy is to outsource these solutions to PCI DSS-compliant payment processors with very specific designs that don't allow credit card information to be processed, stored or transmitted on your DMS.

These designs employ the use of 'tokenized' responses to provide card transaction integration with the ADP DMS. We believe this is a value that competing solutions do not offer. These tokens use non-sensitive information to transact the approval/denial messages that are tied to the appropriate account in your DMS. In the ADP solution, no cardholder information is ever stored, processed or transmitted on the ADP DMS.

PCI compliance is your responsibility; ADP cannot deliver it for you. Compliance is not a one-time event but something you must maintain, like renewing

license plates every year. For some dealers there can be quarterly assessment requirements.

If you accept credit cards for payment, ADP recommends that you engage your legal counsel and/or a PCI Qualified Security Assessor (QSA) consultant to define a PCIDSS compliance plan that suits your dealership.

***FOR MORE INFORMATION**

For more information, visit the official PCI web site. It includes comprehensive details of the PCI DSS, PTS validated readers, certified QSAs and more. It can be found at: <https://www.pcisecuritystandards.org>

The foregoing is provided for information purposes only and is not intended as legal advice. Therefore, it is imperative that you contact your legal counsel to fully understand the effects the PCI-DSS requirements may have on your dealership's operations.