

DATA SECURITY Bulletin



V7 PCI Compliance Update

Radiant Systems engaged Coalfire to complete a full audit of CP V7.5.17 against version 1.2 of the PCI Payment Application Data Security Standards (PA-DSS). As per our standard process, we will then immediately start the process for CPV7.5.18 listing. Keeping our most recent releases listed on the PCI website is a Radiant systems core practice. This is a continual process, and is an inherent part of our release planning. Radiant works closely with our security assessors to ensure that every release adheres to PCI standards. We also follow PCI instructions to ensure that even minor releases do not impact our PCI status.

Previously, CP V7 was listed on the PCI website as validated against Payment Applications Best Practices 1.3 (a preceding standard to PA-DSS 1.2). The PABP standards have expired, thus PCI moved the CP v7 listing to the 'Acceptable for Pre-existing Deployments' tab of the PCI website. The process of completing this most recent audit of CP V7.5.17 has taken longer than expected for many reasons, most of which stem from a considerable backlog within the PCI Council to review and approve compliance reports for all vendors. Please be assured that Radiant, Coalfire, and the PCI Council are doing everything to turn around all compliance reports as quickly as possible.

Based on the completed application testing, process and documentation review, Coalfire will be submitting a report of validation on CP V7.5.17 within the next two to three weeks. Presently, we expect that validation to be successful and approved by the PCI Council. Please be advised that the Council is still experiencing a considerable backlog, and approval turnaround could take a couple of months.

We understand this lag causes questions and concern. To help address those questions, please refer to these documents [PCI PA-DSS Program Guide](#) and the [Visa FAQ dated November 6th 2009](#). Both documents clarify that the expiration date of a standard does not invalidate existing deployments of that application.

If a customer already has v7.5.12 or newer installed, the application is PCI compliant or in the validation process. If you have a new site implementation scheduled immediately and have concerns about PCI compliance, please contact datasecurity@radiantsystems.com. We expect the v7 validation report to be approved by the PCI council, and we expect that approval to be published within 10-12 weeks.

FACTA Reminder

We have spent much time discussing PCI standards for all merchant locations accepting credit cards. Becoming PCI compliant is a measured way to greatly improve the security posture of your store. However, data security is not a point in time activity, but an ongoing objective. And PCI standards will never take the place of federal or state laws. Many merchants are aware of the FACTA law, but in case you are not please read below for very relevant information on how you can protect yourself from potential lawsuit or security breach:

The Fair and Accurate Credit Transactions Act (FACTA) of 2003 added new sections to the federal Fair Credit Reporting Act (FCRA) primarily to help consumers fight identity theft. It focused on accuracy, privacy, and limits on sharing consumer information - including credit card information. FACTA mandated all machine generated debit or credit card receipts printed after December 4, 2006 cannot contain more than the last 5 digits of the card, nor can they show the expiration date of the card.

CounterPoint introduced standard receipts that only show the last 4 digits of the credit card number and do not show expiration date beginning with version 8.3.5 & 7.5.12. Please note that if your customer created a custom receipt prior to upgrading to either of these releases, that receipt was not updated in order to avoid overwriting the customization.

It is imperative that all merchants specifically check their customer receipts to ensure they are showing only

the last five digits or less of any card number and are not showing the expiration date at all. It may be necessary to rebuild custom receipts using a current stock receipt template to ensure proper card number masking. Additionally, merchants should review their customer receipts periodically to ensure changes made over time do not violate FACTA.

For more information regarding this legislation, please visit: <http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf>