FACTS about PCI and Payment Application Data Security Standards

Who is affected? Any merchant using Payment Application software (any merchant that stores, processes, or transmits an Account Number--credit or debit)

How did this come about?

- In 2001, Visa USA mandated all merchants accepting Visa credit cards comply with their Cardholder Information Security Program (CISP). Later, Visa developed Payment Application Best Practices (PABP) for software vendors to improve the security in their credit card application software. Software vendors went through costly and lengthy independent assessment processes to become "PABP Validated". Visa then listed companies (and their new software versions) that met PABP standards on their website.

- In late 2007, Visa announced Payment Application Security Mandates, a series of five deadlines that began January 2008. Phase IV, effective 10/1/09, stated "VNPs (VISA Net Processors) and agents must decertify all vulnerable payment applications". Phase V, effective 7/1/10, stated "Acquirers must ensure their merchants, VNPs, and agents use only PABP-compliant applications". ***This meant that as of October 1, 2009, merchants not using Payment Application software on Visa's "Validated" list could become DECERTIFIED.***

- In late 2008, the Payment Card Industry created a Security Standards Council (PCI-SSC), which adopted Visa's PABP, released a new standard called the Payment Application Data Security Standard (PA-DSS), and began reporting Validation. **The PA-DSS list replaces any previously established standard and Visa's PABP list, available at:** https://www.pcisecuritystandards.org/security_standards/vpa/

What should I do?

1. **Upgrade immediately to a Validated software version, or de-install the integrated Payment Application software.** Every day you wait is another day that you expose your customers to a potential security breach and you to significant fines from your payment processor. If upgrading is not an option, or a validated version is not available, immediately have the integrated payment application de-installed, insure all records and files pertaining to the integrated payment application are deleted (this portion can only be done by a professional), and install non-integrated standalone payment authorization devices. Regardless of this exposure, you may be decertified from using Visa or any form of Credit Cards. However, even using an application on the validated list does not ensure "compliance" with PA-DSS, as there are 12 major requirements. **Your next highest priorities include…**

2. **Separate POS Firewall & Antivirus.** Insure a properly configured, premium Firewall is installed between the POS Network and internal network zone, with an Antivirus software subscription (both should be software update capable). ***The POS must be treated as a demilitarized zone (DMZ) from any internal network zone, by using a separate POS Firewall****.*

3. **Change IDs & Passwords.** Change from default vendor passwords to one unique to site; *configure to not allow remote management of an internet router.*

4. **Database backups.** Secure and validate on hard drives and on network. If "logging" is enabled (for troubleshooting), delete log as soon as troubleshooting is completed.

5. **Start focusing on the other remaining responsibilities of PA-DSS, as there are 12**. Using software on the PA-DSS Validated list does not make you compliant. Software companies and POS vendors can provide and install software that has been "Validated", but neither can perform the many other tasks and responsibilities you are required to meet PA-DSS compliance. Since you, as the Merchant, are responsible for achieving compliance with PA-DSS, take full advantage of the assistance a POS vendor can provide in the practice of following PA-DSS. For more on these requirements: https://www.pcisecuritystandards.org/

An abbreviated 2 page overview of your requirements is available on the DCRS web site (or contact your DCRS Sales Representative for a copy)

What are my risks if I do not act?

1. **Fines and Audits**. It takes months before a payment processor becomes aware of a credit breach. If a credit breach is traced back to a site using software that is not "validated", significant fines will be assessed (tens of thousands of dollars) and annual forensic audits will be required (typically around $10,000 per year), at a minimum.
2. **Lose the ability to accept Visa or any form of Credit Cards**. A site that has not acted on the Visa Mandate may be prevented from accepting Visa or any form of Credit Cards.

What should I expect in the future?

This is not going away. PCI has now defined a 24 to 36 month lifecycle process for changes, and they will revise the requirements every 2 years. Software versions listed on PA-DSS are valid for only 1 year and each require not only an annual revalidation, a process which is very costly, but also a listing fee from the Software vendor on each version's "Annual Revalidation date". **Based on this and the other PA-DSS requirements, in order to maintain your contractual agreements with your Credit Card Issuers, set your expectations that an UPGRADE to the LATEST VERSION of software may be required on a 24 to 36 month cycle. This is not a "legal" requirement—it is your contractual requirement between YOU and your Credit Card Issuer.** https://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf

IF YOUR POS VENDOR IS NOT ADDRESSING PCI SECURITY ISSUES WITH YOU……YOU MAY NEED A NEW POS VENDOR