

Nine Questions to Ask Your Point-of -Sale (POS) Vendor



One aspect of protecting cardholder data and complying with the Payment Card Industry Data Security Standard (PCI DSS) is ensuring that the software you use to accept payment cards is secure. However, it's important to remember that a secure payment application is only one aspect of that security. To protect your business and your customers from payment card theft, you must comply with all 12 requirements of the PCI DSS. This document will arm you with the questions you need to ask your payment application vendor to make sure your payment acceptance system is secure, an explanation of why each question is important and what kind of answer you should expect from a vendor.

1. Is your Point-of-Sale (POS) system compliant with Visa's Payment Application Best Practices (PABP) or the Payment Application Data Security Standard (PA-DSS)?

The Payment Application Data Security Standard (PA-DSS) and Visa's Payment Application Best Practices (PABP) were created to ensure that software vendors create secure payment applications to help prevent the theft of cardholder information.

Visa has announced that all merchants must utilize a PA-DSS compliant payment application by July 1, 2010.

The use of a PA-DSS compliant system helps reduce the risk of a credit card breach, however, it's important to note that PCI DSS compliance requires more than just the use of such an application.

2. How is remote access granted to the Point-of-Sale (POS) systems?

Many POS application vendors use remote access to support their applications. Remote access applications allow a user to remotely manage a system from elsewhere, over the Internet.

A large number of credit card compromises occur due to insecure remote access applications. Some hacking communities post many payment applications' default log-in credentials on the Internet. With these credentials, a hacker has nearly unbridled access to a merchant's payment application and the cardholder data that flows through it.

Remote access applications should only be enabled for the vendor when they need it and not left open at all times. In addition, passwords and usernames utilized for remote access should be unique to your business, sufficiently complex and rotated every 90 days. Two-factor authentication must also be used.

3. Will a hardware-based firewall be supplied? If so, is inbound and outbound access restricted?

A hardware-based firewall is a physical device that sits between the Internet and your network and directs the traffic entering or exiting your network. A properly configured firewall should block all access to your POS system originating from the Internet while allowing the system to communicate with legitimate locations, such as your merchant bank, for processing.

The router or modem provided by your Internet Service Provider (ISP) is not a firewall, and POS application vendors do not typically provide a firewall. Usually, the merchant is responsible for installing and maintaining a firewall to protect their system and achieve compliance requirements.

4. Is an anti-virus and/or anti-malware application installed on the systems?

Attackers today often utilize malicious applications, such as viruses or malware, to gain access to POS systems and capture credit card data. Anti-virus and anti-malware applications detect, alert on, and remove these malicious applications.

A common POS system usually includes a backend server and one or more POS terminals. EVERY computer must have anti-virus and anti-malware applications installed on it.

5. Who is responsible for updates to the Point-of-Sale (POS) systems?

Updates or patches to a POS system's software help maintain its security. Although a POS vendor may keep their own application updated, additional updates such as operating system updates and new anti-virus definitions are also required.

It is important to clarify who, you or the vendor, is responsible for these updates.

6. Do you monitor security and other system event logs on a regular basis for unusual or malicious activity?

All PA-DSS compliant systems generate data logs to provide an audit trail that helps in identifying a potential breach. For example, if an attacker accesses your POS system, a log will be generated by the system identifying unusual activity.

It is probable that your POS vendor does not review these logs on a consistent basis. Often, vendors will only review logs to diagnose system errors such as stability or performance issues. If the POS vendor does not monitor security and other system event logs regularly, it is the merchant's responsibility to review these logs for suspicious activity on a consistent basis. Many security companies, such as Trustwave, offer log monitoring services that automate this task and alert you to suspicious activity.

7. Are system account usernames and passwords unique to my location?

POS systems use system accounts to run the applications present on the computer. Unfortunately, many vendors configure POS systems with default vendor-supplied usernames and passwords.

Attackers often discover these default usernames and passwords and use them to log-in to payment applications. As with remote access credentials, system account passwords and usernames should be unique to your business, sufficiently complex and rotated every 90 days.

8. I need to upgrade to a PA-DSS compliant version of your Point-of-Sale (POS) system. How can I ensure restricted credit card data will be removed?

Non-compliant POS systems often retain restricted credit card data on the system hard drive. While upgrading to a PA-DSS compliant application ensures that an application will not store restricted credit card data for future transactions, many times the data stored by a legacy application is overlooked during installation.

Many POS vendors claim that restricted data will be removed automatically during the upgrade process. However, Trustwave recommends that system hard drives are replaced and old hard drives containing restricted data are securely wiped and destroyed..



9. Do you have procedures in place if my Point-of-Sale (POS) system is breached?

A computer breach must be treated like any other crime scene; evidence must be preserved in its current form. A POS vendor will need to take action to contain a breach in order to prevent further loss of credit card data, such as card-number, magnetic stripe and other data

Given the sensitivity necessary in the preservation of evidence, the initial actions taken by the POS vendor are of grave importance. Visa Inc. has published a document, What To Do If Compromised, to assist merchants if a breach does occur (see http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf).

About Trustwave

Trustwave is the leading provider of on-demand and subscription-based information security and payment card industry compliance management solutions to businesses and government entities throughout the world. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its flagship TrustKeeper® compliance management software and other proprietary security solutions. Trustwave has helped more than 30,000 organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructure, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, Africa, China and Australia. For more information, visit <https://www.trustwave.com/>.

