



PCI Compliance Self-Assessment Questionnaire

4 Sep 2023 / Russ Trantow

Complete

Score	1 / 1 (100%)	Flagged items	4	Actions	0
-------	---------------------	---------------	----------	---------	----------

Conducted on 04.09.2023 16:09 PST

Prepared by Russ Trantow

Location 1090 Pleasant Grove Blvd,
Rosevill Blvd, CA, 95678

Flagged items

4 flagged

Inspection / Common PCI DSS Control Failures

Did you check for for inadequate access controls due to improperly installed point-of-sale (POS) systems, allowing malicious users in via paths intended for POS vendors?

Yes

Inspection / Common PCI DSS Control Failures

Checked for poorly coded web applications that could result in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the website?

Yes

Inspection / Common PCI DSS Control Failures

Checked for missing and outdated security patches?

Yes

Security Patch as of Sept 1, 2023 is up-to-date. See attached file for patch notes

[Security Patch Notes Sept 1, 2023.pdf](#)

Inspection / Common PCI DSS Control Failures

Checked for adequate logging protocols?

Yes

Common PCI DSS Control Failures

4 flagged

Storage of sensitive authentication data (SAD), such as track data, after authorization.

Yes

Is your system storing this data? If so, are you aware of it?

Did you check for for inadequate access controls due to improperly installed point-of-sale (POS) systems, allowing malicious users in via paths intended for POS vendors?

Yes

Default system settings and passwords were changed when the system was installed?

N/A

Passwords to change next Quarter. Expected on Oct 6, 2023.

Unnecessary and insecure services removed or secured when the system was installed?

N/A

Checked for poorly coded web applications that could result in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the website?

Yes

Checked for missing and outdated security patches?

Yes

Security Patch as of Sept 1, 2023 is up-to-date. See attached file for patch notes

[Security Patch Notes Sept 1, 2023.pdf](#)

Checked for adequate logging protocols?

Yes

Checked for adequate monitoring? (via log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems)?

Yes

POS Vendor System's Security (Ask POS Vendor)

Have default settings and passwords been changed on the systems and databases that are part of the POS system?

N/A

Passwords to change next Quarter. Expected on Oct 6, 2023.

Do you access my POS system remotely?

No

remote access is strictly prohibited

Have all unnecessary and insecure services been removed from the systems and databases that are part of the POS

N/A

system?

Not applicable

Is my POS software validated to the Payment Application Data Security Standard (PA-DSS)?

Yes

Does my POS software store sensitive authentication data, such as track data or PIN blocks?

N/A

Does my POS software store primary account numbers (PANs)?

N/A

Will you document the list of files written by the application with a summary of each file's contents to verify that the above-mentioned, prohibited data is not stored?

Yes

Does my POS software enforce complex and unique passwords for all user access?

N/A

Can you confirm that you do not use common or default passwords for access to my system and other merchant systems you support?

Yes

Have all the systems and databases that are part of the POS system been patched with all applicable security updates?

Yes

Passwords to change next Quarter. Expected on Oct 6, 2023.

[Security Patch Notes Sept 1, 2023.pdf](#)

Is the logging capability turned on for the systems and databases that are part of the POS system?

Yes

If prior versions of my POS software stored sensitive authentication data, has this feature been removed during current updates to the POS software? Was a secure wipe utility used to remove this data?

N/A

Cardholder Data

1 / 1 (100%)

Payment brand rules allow for the storage of primary account number (PAN), expiration date, cardholder name, and service code.

Is the storage of this data absolutely necessary for the business and its purpose? State why the data should be stored or eliminated.

No. The data is not needed for any further process after customer transaction.

Is the risk of having the data compromised worth the effort to store it?

N/A

Are the additional PCI DSS controls that need to be applied to protect the data worth the continued storage of this data?

N/A

Are the ongoing maintenance efforts to remain PCI DSS compliant over time worth the continued storage of this data?

N/A

The cardholder data that NEEDS to be stored are properly consolidated and and isolated through proper network segmentation



Compliance Officer Sign-off

Full name and signature of Compliance Officer in-charge

Russ Trantow

Russ Trantow
14.09.2023 16:44 PST

Media summary

[Security Patch Notes Sept 1, 2023.pdf](#)

[Security Patch Notes Sept 1, 2023.pdf](#)