**Murphy-Hoffman Company**

PCI Architecture Workshop

Version 1.0

August 31, 2017

# Version Control

|  |  |
| --- | --- |
| NIST SP800-53 Audit Plan Assessment | |
| Client Name | Murphy-Hoffman Company |
| Client Contact | Eddie Zuniga, PMO Manager |
| Document Issue No | 1.0 |
| Author(s) | Kylen Griffin – Governance, Risk & Compliance |
| Reviewed by: | Keith Knerr – PCI QSA |
| Project Manager | Alexis Hayob – Project Manager |
| Delivery Date | August 31, 2017 |
| Data Classification | Client Confidential |

|  |  |  |  |
| --- | --- | --- | --- |
| NIST SP800-53 Audit Plan Assessment Revision History | | | |
| Version | Description | Author | Date |
| 1.0 | Initial Version | Kylen Griffin | August 31, 2017 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Version Control 2](#_Toc492028048)

[Executive Summary 4](#_Toc492028049)

[Background 4](#_Toc492028050)

[Goals & Objectives 4](#_Toc492028051)

[Findings and Recommendations 5](#_Toc492028052)

[Original Plan – Remote Desktop 5](#_Toc492028053)

[Curbstone Recommended Plan – Tablet Plan 5](#_Toc492028054)

[Card Not Present Plan – PAX S300 Terminal Plan 6](#_Toc492028055)

[Conclusion 7](#_Toc492028056)

# Executive Summary

## Background

Murphy-Hoffman Company (“MHC”) is in the process of implementing a new credit card payment system and needs to ensure their current design proposals are PCI compliant. MHC has requested Fishtech Group, LLC (“Fishtech”) to perform a PCI Architecture Workshop to go over the following three options:

* RDP Sessions
* Forward Proxy
* iFrame

MHC brought in Fishtech to perform a PCI workshop to discuss these three options and other unknown options to minimize the PCI scope as much as possible and gather information to develop a high level strategic roadmap of the options. MHC currently has partnered with Curbstone Corporation (“Curbstone”) to provide credit card integration with the existing MHC AS/400 platform. MHC is utilizing the AS/400 platform to perform point of sales, refund and other customer facing activity. Curbstone has a desired implementation that will additionally be discussed utilizing tablets for the credit card inputs.

## Goals & Objectives

The goal of this project is to validate the current architecture designed developed by MHC and make recommendations to ensure the environment is PCI compliant. In addition, Fishtech will make recommendations to reduce the PCI footprint.

# Findings and Recommendations

## Original Plan – Remote Desktop

During the PCI Workshop MHC and Fishtech discussed the proposed architecture designs for the MHC project. These were using the PC to input credit card information through a RDP Sessions, a Forward Proxy, and finally an iFrame. It was concluded that the RDP session would be the best answer out of these three. But this proposed architecture design would have placed the entire computer under scope for PCI DSS. This option cost would include the cost of the RDP license in addition to the configuration of virtual LANs (“VLANs”) throughout the enterprise to keep the computers at the locations as segregated as possible.

This option would take the longest to completely implement since it would require a for all of the computers that process the credit card information a full SAQ D, which is the self-assessment questionnaire D that contains the entire PCI DSS standard. Since all of the computer would be in scope the amount of work that would be involved. This would require items listed in the SAQ C V/T below in addition to computer hardening, logging and monitoring, quarterly vulnerability scans, annual penetration tests, as well as other items. The following PCI DSS requirements make up the SAQ D.

* Requirement 1: Install and maintain a firewall configuration to protect data
* Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
* Requirement 3: Protect stored cardholder data
* Requirement 4: Encrypt transmission of cardholder data across open, public networks
* Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
* Requirement 6: Develop and maintain secure systems and applications
* Requirement 7: Restrict access to cardholder data by business need to know
* Requirement 8: Identify and authenticate access to system components
* Requirement 9: Restrict physical access to cardholder data
* Requirement 10: Track and monitor all access to network resources and cardholder data
* Requirement 11: Regularly test security systems and processes
* Requirement 12: Maintain a policy that addresses information security for all personnel

## Curbstone Recommended Plan – Tablet Plan

Further discussions were held to find an architecture design that would keep the PCI scope as small as possible. It was discovered through the workshop that Curbstone had a reference architecture that utilized tablets to enter the credit card data instead of the computer. This design would keep the computer out of PCI DSS scope and would allow for the easiest path towards complete PCI DSS compliance. This option would just include the cost of the mobile device management license, and tablet cost, and configuring of separate wireless VLANs.

The PCI DSS reporting requirements for this option would be for the systems in scope which would be the tablets, and any network devices those tablets touch, SAQ C V/T, which is a self-assessment questionnaire that covers the following PCI DSS Requirements:

* Requirement 1: Install and maintain a firewall configuration to protect data
* Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
* Requirement 3: Protect stored cardholder data
* Requirement 4: Encrypt transmission of cardholder data across open, public networks
* Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
* Requirement 6: Develop and maintain secure systems and applications
* Requirement 7: Restrict access to cardholder data by business need to know
* Requirement 9: Restrict physical access to cardholder data
* Requirement 12: Maintain a policy that addresses information security for all personnel

## Card Not Present Plan – PAX S300 Terminal Plan

One final potential architecture design was also introduced and talked about in great lengths although more discussions with TSYS, the company that is MHC processor to determine if there is any validity to the design. This design would entail utilizing the PAX S300 terminals to input all credit cards including card not present. The design might throw off some flags and/or alerts in the TSYS system so further testing and validation would need to occur if this is the selected design going forward. There would be items that MHC would like to gather potentially not available if this design is implemented but that would be a business decision for MHC. This option’s cost would be the additional purchase of the PAX S300 devices and TSYS assistance to ensure that no unnecessary alerts are generated.

While this option would require the least amount of work to achieve compliance, it would still need to be vetted through TSYS and business processes to ensure that the solution would be valid. During the workshop, we could not get TSYS to verify that this would be a legitimate option and will be treated as an invalidated option for the purpose of this report.

# Conclusion

As of this report, it is the opinion of the author that MHC should start with the Curbstone recommended plan and work towards the original plan since it would require a lengthy process to complete the compliance tasks for the original plan. The time estimate for the Curbstone recommended plan would be in the range of three to six months to achieve compliance, while the original plan would be in the range of eighteen to twenty-four months to achieve compliance, in addition to the staff that would be required for the original plan.

This workshop summary is just the first step that MHC will be taking to address their PCI DSS compliance. Starting on September 5, 2017, there will be a full PCI DSS gap assessment done on the MHC enterprise to see how well existing business processes, procedures and technology address the current PCI DSS standard. The plans from this document will be included as inputs into that overall gap assessment and more in-depth recommendations will be made in the gap assessment deliverable for the original plan and the Curbstone recommended plan.