



Payment Card Industry (PCI) Payment Application Data Security Standard

Requirements and Security Assessment Procedures

Version 1.2
October 2008

Table of Contents

Instructions and Content for Report on Validation	ii
PA-DSS Requirements and Security Assessment Procedures	1
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data	1
2. Protect stored cardholder data	8
3. Provide secure authentication features.....	11
4. Log payment application activity.....	13
5. Develop secure payment applications	16
6. Protect wireless transmissions	23
7. Test payment applications to address vulnerabilities.....	25
8. Facilitate secure network implementation	26
9. Cardholder data must never be stored on a server connected to the Internet.....	26
10. Facilitate secure remote software updates.....	27
11. Facilitate secure remote access to payment application.....	28
12. Encrypt sensitive traffic over public networks.....	32
13. Encrypt all non-console administrative access.....	33
14. Maintain instructional documentation and training programs for customers, resellers, and integrators.....	33
Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment.....	35
Appendix C: Attestation of Validation.....	41

Instructions and Content for Report on Validation

This document is to be used by PA-QSAs as the template for creating the Report on Validation. All PA-QSAs must follow instructions in this document for report content and format when completing a Report on Validation.

The Report on Validation should contain the following information as a preface to the detailed Requirements and Security Assessment Procedures:

1. Description of Scope of Review

- Describe scope of review coverage, per the Scope of PA-DSS section above
403 Labs, LLC (403 Labs) performed a PA-DSS assessment against Sensible Cinema 2009, a cinema ticketing and concessions management and POS application.
- Timeframe of validation
403 Labs began the assessment on October 8, 2008, and concluded it on July 3, 2009.
- Statement of Compliance
403 Labs recommends that Sensible Cinema 2009 obtain a rating of COMPLIANT with the PA-DSS v1.2.
- PA-DSS version used for the assessment
403 Labs used the PA-DSS v1.2 for this assessment
- List of documentation reviewed
PA-DSS Implementation Guide
Revision History including change management information
Code review output
Card Data Flow chart

2. Executive Summary

Include the following:

- Product Name
Sensible Cinema

- Product Version and related platforms covered
2009 v3.0.8

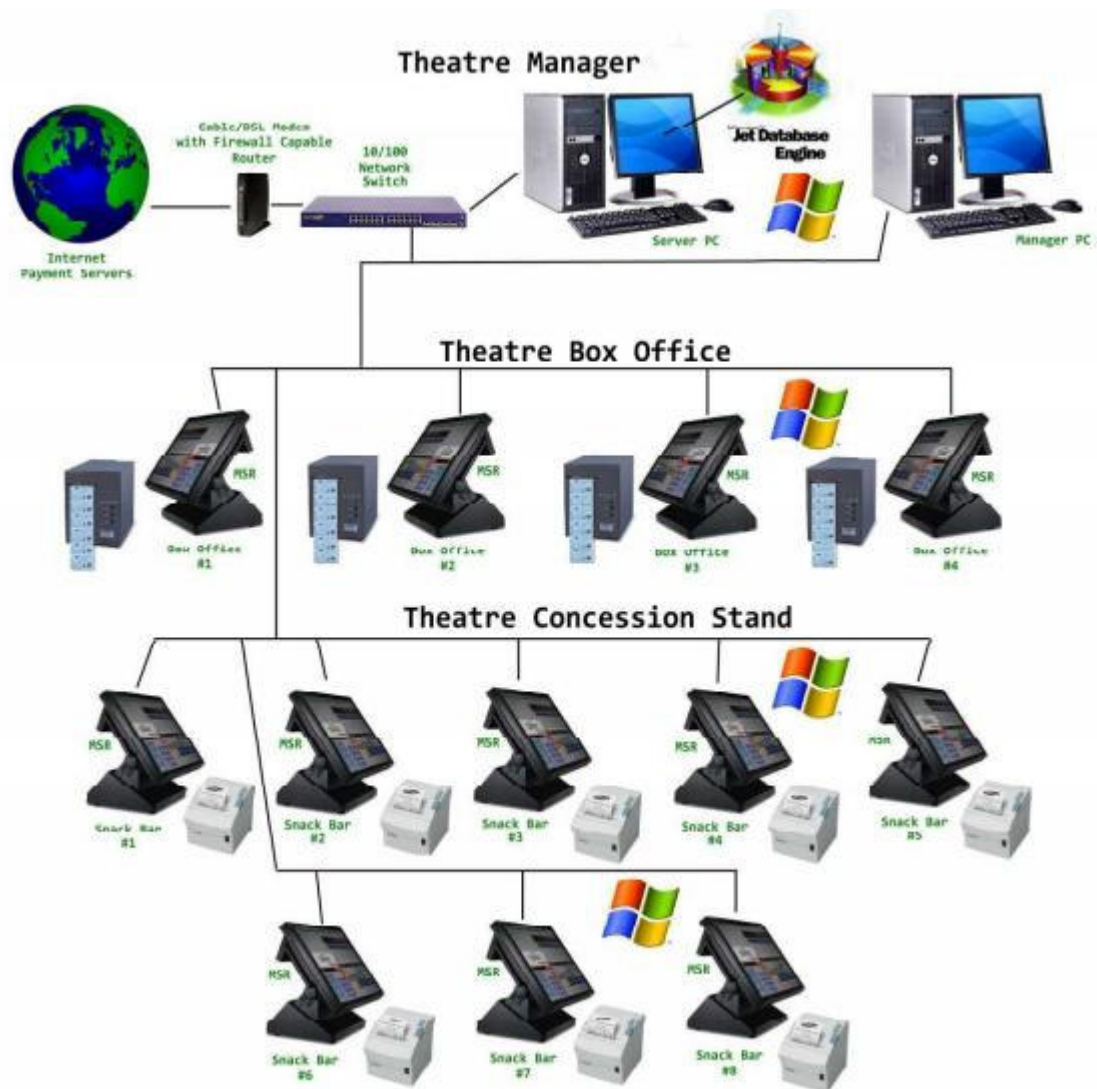
- List of resellers and/or integrators for this product
None. Sensible Cinema did not use resellers or integrators

- Operating system(s) with which the payment application was tested
Windows XP SP3

- Database software used or supported by the payment application
Sensible Cinema used MS Access database files, but did not require the full application.

- Brief description of the payment application/family of products (2-3 sentences)
Sensible Cinema is a full-service cinema and concessions management application that accepts credit cards for payment. Sensible Cinema communicates transactions to Mercury Payment Systems for authorization and settlement and did not store cardholder data.

- Network diagram of a typical implementation of the payment application (not necessarily a specific implementation at a customer's site) that includes, at high level:
 - Connections into and out of a customer's network
 - Components within the customer's network, including POS devices, systems, databases, and web servers as applicable
 - Other necessary payment application/components, as applicable



Sensible Cinema operates on a server, which communicates via HTTPS with the payment processor. Sensible Cinema can include other PCs including terminals to sell tickets or concessions and typical setups include a manager's PC with access to reporting and management functions.

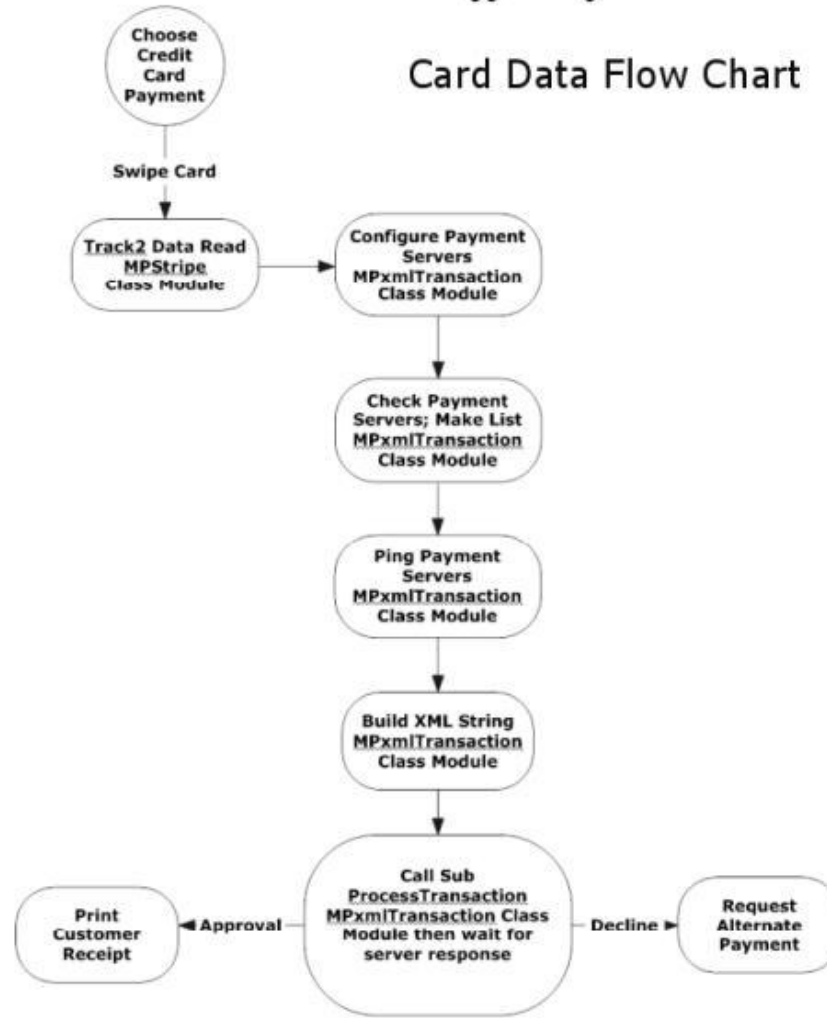
- Description or diagram of each piece of the communication link, including (1) LAN, WAN or Internet, (2) host to host software communication, and (3) within host where software is deployed (for example, how two different processes communicate with each other on the same host)

Sensible Cinema consists of client and server components that communicate over Windows Networking or over inter-process communication, if the two components reside on the same host. Sensible Cinema communicates over HTTPS with the payment processor over the Internet for all communications.

- A dataflow diagram that shows all flows of cardholder data, including authorization, capture, settlement, and chargeback flows as applicable

Sensible Cinema Software *Box Office for Windows*

Card Data Flow Chart



Sensible Cinema uses HTTPS to communicate with the payment processor for all data flows, including authorization, settlement, and chargeback.

Brief description of files and tables that store cardholder data, supported by an inventory created (or obtained from the software vendor) and retained by the PA-QSA in the work papers—this inventory should include, for each cardholder data store (file, table, etc.):

- List of all elements of stored cardholder data
- How data store is secured
- How access to data store is logged

Sensible Cinema did not show evidence of stored cardholder data under any circumstances.

- List all payment application related software components, including third-party software requirements and dependencies
Sensible Cinema requires a current Windows operating system to function
- Description of payment application's end to end authentication methods, including application authentication mechanism, authentication database, and security of data storage
Sensible Cinema requires authentication at the application layer for all components and the PA-DSS Implementation Guide requires authentication at the operating system level.
- Description of role of payment application in a typical implementation and what other types of payment applications are necessary for a full payment implementation
Sensible Cinema did not require any other payment applications to function, and acted as the point of sale for all transactions.
- Description of the testing laboratory
403 Labs tested Sensible Cinema on a Windows XP machine with current security patches in a PCI DSS-compliant network using a Fortigate firewall and ClamWin anti-virus software.
- Description of the typical customer that this product is sold to (for example, large, small, whether industry-specific, Internet, brick-and-mortar) and vendor's customer's base (for example, market segment, big customer names).
Sensible Cinema is sold to cinemas who accept credit cards for tickets and concessions.
- Definition of vendor's versioning methodology, to describe/illustrate how vendor indicates major and minor version changes via their version numbers, and to define what types of changes the vendor includes in major and minor version changes.
Sensible Cinema uses major and minor versions and build versions to designate specific releases. Major versions represent the addition of significant new features in the application. Minor versions typically include features requested by customers and not released on a specific schedule. Build versions denote a specific major and minor version with changes to enhance existing features, bug fixes, or cosmetic changes.

3. Findings and Observations

- All PA-QSAs must use the following template to provide detailed report descriptions and findings See below.
- Describe tests performed other than those included in the testing procedures column.
N/A. 403 Labs used only test procedures in the PA-DSS.

4. Contact Information and Report Date

- Software vendor contact information (include URL, phone number, and e-mail address)
Rusty Gordon
Sensible Cinema Software
7216 Sutton Place
Fairview, TN 37062
info@sensiblecinema.com
www.sensiblecinema.com
- PA-QSA contact information (include name, phone number and e-mail address)
Jacob Ansari
403 Labs, LLC
877.403.5227 x215
jansari@403labs.com
- PA-QSA Quality Assurance (QA) primary contact information (include primary QA contact's name, phone number and e-mail address)
D.J. Vogel
403 Labs, LLC
877.403.5227 x213
djvogel@403labs.com
- Date of report
July 3, 2009

PA-DSS Requirements and Security Assessment Procedures

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data				
<p>1.1 Do not store sensitive authentication data after authorization (even if encrypted):</p> <p>Sensitive authentication data includes the data as cited in the following Requirements 1.1.1 through 1.1.3.</p> <p>PCI Data Security Standard Requirement 3.2</p> <p><i>Note: By prohibiting storage of sensitive authentication data after authorization, the assumption is that the transaction has completed the authorization process and the customer has received the final transaction approval. After authorization has completed, this sensitive authentication data cannot be stored.</i></p>	<p>1.1 If sensitive authentication data (see 1.1.1–1.1.3 below) is stored prior to authorization and then deleted, obtain and review methodology for deleting the data to determine that the data is unrecoverable.</p> <p>For each item of sensitive authentication data below, perform the following steps after completing numerous test transactions that simulate all functions of the payment application, to include generation of error conditions and log entries.</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema did not store sensitive authentication data.</p>		
<p>1.1.1 After authorization, do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</p> <p><i>In the normal course of business, the following data elements from the</i></p>	<p>1.1.1 Use forensic tools and/or methods (commercial tools, scripts, etc.)¹ to examine all output created by the payment application and verify that the full contents of any track from the magnetic stripe on the back of the card are not stored after authorization. Include the following types of files (as well as any other output generated by the</p>	<p>403 Labs used forensic tools and reviewed system configuration settings, which did not show evidence that Sensible Cinema stored magnetic stripe data anywhere except in volatile memory. Specifically, 403 Labs examined the following:</p> <ul style="list-style-type: none"> ▪ Incoming transaction data -403 Labs examined incoming transaction data, which did not show evidence that Sensible 		

¹ Forensic tool or method: A tool or method for uncovering, analyzing and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly. In the case of forensic tools or methods used by PA-QSAs, these tools or methods should accurately locate any sensitive authentication data written by the payment application. These tools may be commercial, open-source, or developed in-house by the PA-QSA.

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p><i>magnetic stripe may need to be retained:</i></p> <ul style="list-style-type: none"> ▪ <i>The accountholder's name,</i> ▪ <i>Primary account number (PAN),</i> ▪ <i>Expiration date, and</i> ▪ <i>Service code</i> <p><i>To minimize risk, store only those data elements needed for business.</i></p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p> <p>PCI Data Security Standard Requirement 3.2.1</p>	<p>payment application):</p> <ul style="list-style-type: none"> ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Non-volatile memory, including non-volatile cache ▪ Database schemas ▪ Database contents 	<p>Cinema stored magnetic stripe data.</p> <ul style="list-style-type: none"> ▪ Transaction logs -403 Labs examined transaction logs, which did not show evidence that Sensible Cinema stored magnetic stripe data. ▪ History files - 403 Labs examined history files, which did not show evidence that Sensible Cinema stored magnetic stripe data. ▪ Trace files - 403 Labs examined trace files, which did not show evidence that Sensible Cinema stored magnetic stripe data. ▪ Non-volatile memory, including non-volatile cache -N/A. Sensible Cinema did not make use of non-volatile memory. ▪ Debugging and error logs - 403 Labs examined debug and error logs, which did not show evidence that Sensible Cinema stored magnetic stripe data. ▪ Audit logs - 403 Labs examined audit logs, which did not show evidence that Sensible Cinema stored magnetic stripe data. ▪ Database schema and tables - 403 Labs examined database files, which did not show evidence that Sensible Cinema stored magnetic stripe data. ▪ Database contents - 403 Labs examined database contents, which did not show evidence that Sensible Cinema stored magnetic stripe data. 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p>1.1.2 After authorization, do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.</p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p> <p>PCI Data Security Standard Requirement 3.2.2</p>	<p>1.1.2 Use forensic tools and/or methods (commercial tools, scripts, etc.)² to examine all output created by the payment application and verify that the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization. Include the following types of files (as well as any other output generated by the payment application):</p> <ul style="list-style-type: none"> ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Non-volatile memory, including non-volatile cache ▪ Database schemas ▪ Database contents 	<p>403 Labs used forensic tools and reviewed system configuration settings, which showed that which did not show evidence that Sensible Cinema accepted or stored card validation codes. Specifically, 403 Labs examined the following:</p> <ul style="list-style-type: none"> ▪ Incoming transaction data - 403 Labs examined incoming transaction data, which did not show evidence that Sensible Cinema accepted or stored card validation codes. ▪ Transaction logs - 403 Labs examined transaction logs, which did not show evidence that Sensible Cinema accepted or stored card validation codes. ▪ History files - 403 Labs examined history files, which did not show evidence that Sensible Cinema accepted or stored card validation codes. ▪ Trace files - 403 Labs examined trace files, which did not show evidence that Sensible Cinema accepted or stored card validation codes. ▪ Non-volatile memory, including non-volatile cache - N/A. Sensible Cinema did not make use of non-volatile memory. ▪ Debugging and error logs - 403 		

² Forensic tool or method: A tool or method for uncovering, analyzing and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly. In the case of forensic tools or methods used by PA-QSAs, these tools or methods should accurately locate any sensitive authentication data written by the payment application. These tools may be commercial, open-source, or developed in-house by the PA-QSA.

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
		<p>Labs examined debug and error logs, which did not show evidence that Sensible Cinema accepted or stored card validation codes.</p> <ul style="list-style-type: none"> ▪ Audit logs - 403 Labs examined audit logs, which did not show evidence that Sensible Cinema accepted or stored card validation codes. ▪ Database schema and tables - 403 Labs examined database files, which did not show evidence that Sensible Cinema accepted or stored card validation codes. ▪ Database contents -403 Labs examined database contents, which did not show evidence that Sensible Cinema accepted or stored card validation codes. 		
<p>1.1.3 After authorization, do not store the personal identification number (PIN) or the encrypted PIN block.</p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p> <p>PCI Data Security Standard Requirement 3.2.3</p>	<p>1.1.3 Use forensic tools and/or methods (commercial tools, scripts, etc.)⁵ to examine all output created by the payment application, and verify that PINs and encrypted PIN blocks are not stored after authorization. Include the following types of files (as well as any other output generated by the payment application).</p> <ul style="list-style-type: none"> ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Non-volatile memory, including 	<p>403 Labs used forensic tools and reviewed system configuration settings, which showed that which did not show evidence that Sensible Cinema accepted or stored PIN or encrypted PIN block data anywhere except in volatile memory. Specifically, 403 Labs examined the following:</p> <ul style="list-style-type: none"> ▪ Incoming transaction data -403 Labs examined incoming transaction data, which did not show evidence that Sensible Cinema accepted or stored PIN or encrypted PIN block data. ▪ Transaction logs -403 Labs examined transaction logs, which did not show evidence that Sensible Cinema accepted or 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	non-volatile cache <ul style="list-style-type: none"> ▪ Database schemas ▪ Database contents 	stored PIN or encrypted PIN block data. <ul style="list-style-type: none"> ▪ History files -403 Labs examined history files, which did not show evidence that Sensible Cinema accepted or stored PIN or encrypted PIN block data. ▪ Trace files -403 Labs examined trace files, which did not show evidence that Sensible Cinema accepted or stored PIN or encrypted PIN block data. ▪ Non-volatile memory, including non-volatile cache - N/A. Sensible Cinema did not make use of non-volatile storage. ▪ Debugging and error logs -403 Labs examined debug and error logs, which did not show evidence that Sensible Cinema accepted or stored PIN or encrypted PIN block data. ▪ Audit logs - 403 Labs examined audit logs, which did not show evidence that Sensible Cinema accepted or stored PIN or encrypted PIN block data. ▪ Database schema and tables - 403 Labs examined database files, which did not show evidence that Sensible Cinema accepted or stored PIN or encrypted PIN block data. ▪ Database contents -403 Labs examined database contents, which did not show evidence that Sensible Cinema accepted or stored PIN or encrypted PIN block data. 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p>1.1.4 Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.</p> <p>PCI Data Security Standard Requirement 3.2</p> <p><i>Note: This requirement only applies if previous versions of the payment application stored sensitive authentication data.</i></p>	<p>1.1.4.a Review the <i>PA-DSS Implementation Guide</i> prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators:</p> <ul style="list-style-type: none"> ▪ That historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the payment application) ▪ How to remove historical data ▪ That such removal is absolutely necessary for PCI DSS compliance 	<p>N/A. 403 Labs reviewed the system configuration settings, interviewed Rusty Gordon - Owner, and observed application function, , which did not show evidence of stored sensitive authentication data.</p>		
	<p>1.4.b Verify the vendor provides a secure wipe tool or procedure to remove the data.</p>	<p>N/A. 403 Labs reviewed the system configuration settings, interviewed Rusty Gordon - Owner, and observed application function, , which did not show evidence of stored sensitive authentication data.</p>		
	<p>1.1.4.c Verify, through the use of forensic tools and/or methods, that the secure wipe tool or procedure provided by vendor securely removes the data, in accordance with industry-accepted standards for secure deletion of data.</p>	<p>N/A. 403 Labs reviewed the system configuration settings, interviewed Rusty Gordon - Owner, and observed application function, which did not show evidence of stored sensitive authentication data.</p>		
<p>1.1.5 Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data,</p>	<p>1.1.5.a Examine the software vendor's procedures for troubleshooting customers' problems and verify the procedures include:</p> <ul style="list-style-type: none"> ▪ Collection of sensitive authentication data only when 	<p>403 Labs observed application function, reviewed the PA-DSS Implementation Guide, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema did not collect sensitive authentication data under any circumstances.</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p>card validation codes or values, and PINs or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.</p> <p>PCI Data Security Standard Requirement 3.2</p>	<p>needed to solve a specific problem</p> <ul style="list-style-type: none"> ▪ Storage of such data in a specific, known location with limited access ▪ Collection of only a limited amount of data needed to solve a specific problem ▪ Encryption of sensitive authentication data while stored ▪ Secure deletion of such data immediately after use 			
	<p>1.1.5.b Select a sample of recent troubleshooting requests from customers, and verify each event followed the procedure examined at 1.1.5.a.</p>	<p>N/A. 403 Labs observed application function, reviewed the PA-DSS Implementation Guide, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema did not collect sensitive authentication data under any circumstances.</p>		
	<p>1.1.5.c Review the <i>PA-DSS Implementation Guide</i> prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators:</p> <ul style="list-style-type: none"> ▪ Collect sensitive authentication only when needed to solve a specific problem. ▪ Store such data only in specific, known locations with limited access. ▪ Collect only the limited amount of data needed to solve a specific problem. ▪ Encrypt sensitive authentication data while stored. 	<p>Sensible Cinema did not permit the collection of sensitive authentication data for troubleshooting.</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	<ul style="list-style-type: none"> ▪ Securely delete such data immediately after use. 			
2. Protect stored cardholder data				
<p>2.1 Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period.</p> <p>PCI Data Security Standard Requirement 3.1</p>	<p>2.1.a Review the <i>PA-DSS Implementation Guide</i> prepared by the vendor and verify the documentation includes the following guidance for customers and resellers/integrators:</p> <ul style="list-style-type: none"> ▪ That cardholder data exceeding the customer-defined retention period must be purged ▪ A list of all locations where the payment application stores cardholder data (so that customer knows the locations of data that needs to be deleted) 	<p>403 Labs reviewed the PA-DSS Implementation Guide, which stated that Sensible Cinema did not store PAN data under any circumstances.</p>		
<p>2.2 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).</p> <p><i>Notes:</i></p> <ul style="list-style-type: none"> ▪ <i>This requirement does not apply to those employees and other parties with a legitimate business need to see full PAN;</i> ▪ <i>This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.</i> <p>PCI Data Security Standard Requirement 3.3</p>	<p>2.2 Review displays of credit card data, including but not limited to POS devices, screens, logs, and receipts, to determine that credit card numbers are masked when displaying cardholder data, except for those with a legitimate business need to see full credit card numbers.</p>	<p>403 Labs observed application function, which showed that Sensible Cinema masked card number display to the last four digits for the following:</p> <ul style="list-style-type: none"> ▪ POS devices, which did not show evidence of the display of full PAN. ▪ Screens, which did not show evidence of the display of full PAN. ▪ Logs, which did not show evidence of the display of full PAN. ▪ Receipts, which did not show evidence of the display of full PAN. 		
<p>2.3 Render PAN, at a minimum, unreadable anywhere it is stored, (including data on portable digital</p>	<p>2.3.a Verify that the PAN is rendered unreadable anywhere it is stored, in accordance with PCI DSS</p>	<p>403 Labs observed application function and reviewed system configuration settings, which did not</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p>media, backup media, and in logs) by using any of the following approaches:</p> <ul style="list-style-type: none"> ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key management processes and procedures. <p>The MINIMUM account information that must be rendered unreadable is the PAN.</p> <p>PCI Data Security Standard Requirement 3.4</p> <p><i>The PAN must be rendered unreadable anywhere it is stored, even outside the payment application.</i></p> <p><i>Note: "Strong cryptography" is defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.</i></p>	<p>Requirement 3.4.</p> <p>2.3.b If the software vendor stores the PAN for any reason (for example, because log files, debugging files, and other data sources are received from customers for debugging or troubleshooting purposes), verify that the PAN is rendered unreadable in accordance with PCI DSS Requirement 3.4.</p>	<p>show evidence that Sensible Cinema stored PAN data.</p> <p>N/A. Sensible Cinema did not collect PAN data under any circumstances.</p>		
<p>2.4 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.</p> <p>PCI Data Security Standard Requirement 3.4.1</p>	<p>2.4 If disk encryption is used, verify that it is implemented in accordance with PCI DSS Requirements 3.4.1.a through 3.4.1.c.</p>	<p>N/A. Disk encryption was not used.</p>		
<p>2.5 Payment application must protect cryptographic keys used for encryption of cardholder data against disclosure and misuse.</p> <p>PCI Data Security Standard</p>	<p>2.5 Verify the payment application protects keys against disclosure and misuse, per PCI DSS Requirement 3.5.1 and 3.5.2.</p>	<p>N/A. No data storage or encryption keys were in use.</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
Requirement 3.5				
<p>2.6 Payment application must implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.</p> <p>PCI Data Security Standard Requirement 3.6</p>	<p>2.6 Verify the payment application implements key-management techniques for keys, per PCI DSS Requirements 3.6.1 through 3.6.8.</p>	N/A. No data storage or encryption keys were in use.		
<p>2.7 Securely delete any cryptographic key material or cryptogram stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations. These are cryptographic keys used to encrypt or verify cardholder data.</p> <p>PCI Data Security Standard Requirement 3.6</p> <p><i>Note: This requirement only applies if previous versions of the payment application used cryptographic key materials or cryptograms to encrypt cardholder data.</i></p>	<p>2.7.a Review the <i>PA-DSS Implementation Guide</i> prepared by the vendor and verify the documentation includes the following instructions for customers and resellers/integrators:</p> <ul style="list-style-type: none"> ▪ That cryptographic material must be removed ▪ How to remove cryptographic material ▪ That such removal is absolutely necessary for PCI DSS compliance ▪ How to re-encrypt historic data with new keys 	N/A. No data storage or encryption keys were in use.		
	<p>2.7.b Verify vendor provides a secure wipe tool or procedure to remove cryptographic material.</p>	N/A. No data storage or encryption keys were in use.		
	<p>2.7.c Verify, through use of forensic tools and/or methods, that the secure wipe tool or procedure securely removes the cryptographic material, in accordance with industry-accepted standards for secure deletion of data.</p>	N/A. No data storage or encryption keys were in use.		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
3. Provide secure authentication features				
<p>3.1 The “out of the box” installation of the payment application in place at the completion of the installation process, must facilitate use of unique user IDs and secure authentication (defined at PCI DSS Requirements 8.1, 8.2, and 8.5.8–8.5.15) for all administrative access and for all access to cardholder data.</p> <p>PCI Data Security Standard Requirements 8.1, 8.2, and 8.5.8–8.5.15</p> <p><i>Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the payment application.</i></p> <p><i>This requirement applies to the payment application and all associated tools used to view or access cardholder data.</i></p>	<p>3.1.a Test the payment application to verify that unique user IDs and secure authentication are required for all administrative access and for all access to cardholder data, in accordance with PCI DSS Requirements 8.1, 8.2, and 8.5.8–8.5.15.</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide, reviewed the system configuration settings, interviewed Rusty Gordon - Owner, and observed application function, which showed that Sensible Cinema required unique usernames and strong passwords, specifically:</p> <ul style="list-style-type: none"> ▪ Users required a unique username ▪ Users must authenticate with a password ▪ Users were instructed to not authenticate with group, shared, or generic passwords ▪ Passwords consisted of at least seven characters in length ▪ Passwords consisted of alphabetic and numeric characters ▪ Passwords that expired every 90 days. ▪ Accounts must not re-use the prior four passwords. ▪ Accounts must lock out after six invalid attempts. ▪ Locked accounts must remain locked out for 30 minutes. ▪ Sessions must time out after 15 minutes of inactivity. 		
	<p>3.1.b Test the payment application to verify the payment application does not use (or require the use of) default administrative accounts for other necessary software (for example, the payment application must not use the</p>	<p>403 Labs observed application function, which showed that Sensible Cinema did not use or require the use of default administrative accounts.</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	administrative account for database software).			
	<p>3.1.c Examine <i>PA-DSS Implementation Guide</i> created by vendor to verify the following:</p> <ul style="list-style-type: none"> ▪ Customers and resellers/integrators are advised against using default administrative accounts for payment application logins (for example, don't use the "sa" account for payment application access to the database). ▪ Customers and resellers/integrators are advised to assign secure authentication to these default accounts (even if they won't be used), and then disable or do not use the accounts. ▪ Customers and resellers/integrators are advised to assign secure authentication for payment applications and systems whenever possible. ▪ Customers and resellers/integrators are advised how to create PCI DSS-compliant secure authentication to access the payment application, per PCI DSS Requirements 8.5.8 through 8.5.15 ▪ Customers and resellers/integrators are advised that changing "out of the box" installation settings for unique user IDs and secure authentication will result in non-compliance with PCI DSS. 	<p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema:</p> <ul style="list-style-type: none"> ▪ Advised against the use of default administrative accounts ▪ Instructed customers to secure and disable these accounts ▪ Instructed customers to assign secure authentication for payment applications and systems° ▪ Advised customers on how to create PCI DSS-compliant passwords specifically: <ul style="list-style-type: none"> ○ Users must require a unique username ○ Users must authenticate with a password ○ Users must not authenticate with group, shared, or generic passwords ○ Passwords must contain at least 7 characters ○ Passwords must consist of alphabetic and numeric characters ○ Passwords must expire every 90 days. ○ Accounts must not re-use the prior 4 passwords ○ Accounts must lock out after 6 invalid attempts ○ Locked accounts must remain locked out for 30 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
		minutes. <ul style="list-style-type: none"> ○ Sessions must time out after 15 minutes of inactivity ▪ Advised customers that not requiring unique usernames and secure authentication would result in non-compliance with the PCI DSS. 		
<p>3.2 Access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication.</p> <p><i>PCI Data Security Standard Requirements 8.1 and 8.2</i></p>	<p>3.2 Examine <i>PA-DSS Implementation Guide</i> created by vendor to verify customers and resellers/integrators are strongly advised to control access, via unique user ID and PCI DSS-compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data.</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema instructed customers to use unique usernames and strong, PCI DSS-compliant secure authentication on PCs, servers, and databases with Sensible Cinema. Sensible Cinema did not use resellers or integrators.</p>		
<p>3.3 Render payment application passwords unreadable during transmission and storage, using strong cryptography based on approved standards</p> <p><i>Note: "Strong cryptography" is defined in PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.</i></p> <p><i>PCI Data Security Standard Requirement 8.4</i></p>	<p>3.3 Examine payment application password files during storage and transmission to verify that passwords are unreadable at all times.</p>	<p>403 Labs observed application function and reviewed the system configuration settings, which showed that passwords were encrypted in transmission and storage.</p>		
<p>4. Log payment application activity</p>				
<p>4.1 At the completion of the installation process, the "out of the box" default installation of the payment application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users.</p>	<p>4.1 Examine payment application settings to verify that payment application audit trails are automatically enabled or are available to be enabled by customers.</p>	<p>403 Labs observed application function and reviewed system configuration settings, which showed that audit trails were enabled by default.</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p><i>PCI Data Security Standard Requirement 10.1</i></p>				
<p>4.2 Payment application must implement an automated audit trail to track and monitor access.</p> <p><i>PCI Data Security Standard Requirements 10.2 and 10.3</i></p>	<p>4.2.a Examine payment application log parameters and verify that logs contain the data required in PCI DSS Requirements 10.2.1 through 10.2.7 and 10.3.1 through 10.3.6.</p>	<p>403 Labs observed log values and interviewed Rusty Gordon - Owner, who confirmed that they contained the following elements:</p> <ul style="list-style-type: none"> ▪ Access to cardholder data - N/A. No access to cardholder data. ▪ Actions undertaken by administrators -Logs recorded actions undertaken by administrators. ▪ Access to audit trails logged - Logs recorded access to audit trails. ▪ Invalid logical access attempts are logged -Logs recorded invalid logical access attempts. ▪ Use of identification and authorization mechanisms - Logs recorded use of identification and authorization mechanisms. ▪ Initialization of audit logs - Logs recorded initialization of audit logs. ▪ Creation and deletion of system-level objects -Logs recorded creation and deletion of system level objects. <p>Additionally, logs contain the following properties:</p> <ul style="list-style-type: none"> ▪ User identification -Logs identified the user in question. 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
		<ul style="list-style-type: none"> ▪ Type of event -Logs indicated the event type ▪ Date and time stamp -Logs recorded a date and time stamp. ▪ Note success or failure -Logs indicated success or failure of the event. ▪ Origination of event -Logs noted the origination of event. ▪ Identify affected resource - Logs identified the affected resource, data, or component 		
	<p>4.2.b If payment application log settings are configurable by the customer and resellers/integrators, or customers or resellers/integrators are responsible for implementing logging, examine <i>PA-DSS Implementation Guide</i> prepared by the vendor to verify the following information is included:</p> <ul style="list-style-type: none"> ▪ How to set PCI DSS-compliant log settings, per PCI DSS Requirements 10.2.1 through 10.2.7 and 10.3.1 through 10.3.6 ▪ That disabling of the logs should not be done and will result in non-compliance with PCI DSS 	<p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema instructed customers to configure logs with the following elements:</p> <ul style="list-style-type: none"> ▪ Access to cardholder data -N/A. No access to cardholder data. ▪ Actions undertaken by administrators -Logs should record actions undertaken by administrators. ▪ Access to audit trails logged - Logs should record access to audit trails. ▪ Invalid logical access attempts are logged -Logs should record invalid logical access attempts. ▪ Use of identification and authorization mechanisms -Logs should record use of identification and authorization mechanisms. ▪ Initialization of audit logs -Logs should record initialization of 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
		<p>audit logs.</p> <ul style="list-style-type: none"> ▪ Creation and deletion of system-level objects -Logs should record creation and deletion of system level objects. <p>Additionally, logs should contain the following properties:</p> <ul style="list-style-type: none"> ▪ User identification -Logs should identify the user in question. ▪ Type of event -Logs should indicate the event type ▪ Date and time stamp -Logs should record a date and time stamp. ▪ Note success or failure -Logs should indicate success or failure of the event. ▪ Origination of event -Logs should note the origination of event. ▪ Identify affected resource -Logs identified the affected resource, data, or component. <p>And</p> <ul style="list-style-type: none"> ▪ Disabling of logs will result in non-compliance with the PCI DSS. <p>Sensible Cinema did not use resellers or integrators.</p>		

5. Develop secure payment applications

5.1 Develop all payment applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices and incorporate information security throughout the software development life cycle. These

5.1 Obtain and examine written software development processes to verify that they are based on industry standards, that security is included throughout the life cycle, and that software applications are developed in accordance with PCI DSS.

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p>processes must include the following: PCI Data Security Standard Requirement 6.3</p>	<p>From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:</p>			
<p>5.1.1 Testing of all security patches and system and software configuration changes before deployment, including but not limited to testing for the following.</p>	<p>5.1.1 All security patches and system and software changes are tested before being deployed, including but not limited to testing for the following.</p>			
<p>5.1.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)</p>	<p>5.1.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)</p>	<p>403 Labs observed code review output, reviewed the Code Review Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema tested software changes and updates against input validation errors.</p>		
<p>5.1.1.2 Validation of proper error handling</p>	<p>5.1.1.2 Validation of proper error handling</p>	<p>403 Labs observed code review output, reviewed the Code Review Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema tested software changes and updates for proper error handling.</p>		
<p>5.1.1.3 Validation of secure cryptographic storage</p>	<p>5.1.1.3 Validation of secure cryptographic storage</p>	<p>403 Labs observed code review output, reviewed the Code Review Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema tested software changes to validate secure cryptographic storage.</p>		
<p>5.1.1.4 Validation of secure communications</p>	<p>5.1.1.4 Validation of secure communications</p>	<p>403 Labs observed code review output, reviewed the Code Review Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema tested software</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
		changes and updates for secure communication.		
5.1.1.5 Validation of proper role-based access control (RBAC)	5.1.1.5 Validation of proper role-based access control (RBAC)	403 Labs observed code review output, reviewed the Code Review Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema tested software changes and updates for proper role-based access control (RBAC).		
5.1.2 Separate development/test, and production environments	5.1.2 The test/development environments are separate from the production environment, with access control in place to enforce the separation.	403 Labs reviewed the network diagram, reviewed the Software Development Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema maintained separate test/development and production environments and maintained this separation with access controls.		
5.1.3 Separation of duties between development/test, and production environments	5.1.3 There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.	N/A. Sensible Cinema had only one owner/employee.		
5.1.4 Live PANs are not used for testing or development.	5.1.4 Live PANs are not used for testing and development, or are sanitized before use.	403 Labs observed revision history and change management documents, reviewed the Software Development Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema did not use live PANs for testing.		
5.1.5 Removal of test data and accounts before production systems become active	5.1.5 Test data and accounts are removed before a production system becomes active.	403 Labs observed revision history and change management documents, reviewed the Software Development Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema removed test data and accounts before activating production systems.		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p>5.1.6 Removal of custom payment application accounts, user IDs, and passwords before payment applications are released to customers</p>	<p>5.1.6 Custom payment application accounts, user IDs, and passwords are removed before payment application is released to customers.</p>	<p>403 Labs observed revision history and change management documents, reviewed the Software Development Procedures, and interviewed Rusty Gordon - Owner, who confirmed that Sensible Cinema removed custom accounts, usernames, and passwords before releasing to customers.</p>		
<p>5.1.7 Review of payment application code prior to release to customers after any significant change, to identify any potential coding vulnerability.</p> <p><i>Note: This requirement for code reviews applies to all payment application components (both internal and public-facing web applications), as part of the system development life cycle required by PA-DSS Requirement 5.1 and PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties.</i></p>	<p>5.1.7.a Confirm the vendor performs code reviews for all application code changes for <i>internal applications</i> (either using manual or automated processes), as follows:</p> <ul style="list-style-type: none"> ▪ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release. 	<p>403 Labs observed code review output, reviewed the Software Development Procedures, and interviewed Rusty Gordon - Owner, who confirmed that</p> <ul style="list-style-type: none"> ▪ Sensible Cinema performed code reviews by individuals knowledgeable in code review techniques and secure coding practices. ▪ Appropriate corrections were implemented prior to release ▪ Code review results were reviewed and approved by management prior to release – N/A. Sensible Cinema consists of only one person. 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	<p>5.1.7.b Confirm the vendor performs code reviews for all application code changes for <i>web applications</i> (using either manual or automated processes) as follows:</p> <ul style="list-style-type: none"> ▪ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. ▪ Code reviews ensure code is developed according to secure coding guidelines such as the <i>Open Web Security Project Guide</i>. (See PA-DSS Requirement 5.2 and PCI DSS Requirement 6.5.) ▪ Appropriate corrections are implemented prior to release. ▪ Code review results are reviewed and approved by management prior to release. 	N/A. Sensible Cinema is not a web application.		
<p>5.2 Develop all web payment applications (internal and external, and including web administrative access to product) based on secure coding guidelines such as the <i>Open Web Application Security Project Guide</i>. Cover prevention of common coding vulnerabilities in software development processes, to include:</p> <p><i>Note: The vulnerabilities listed in PA-DSS Requirements 5.2.1 through 5.2.10 and in PCI DSS at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when</i></p>	<p>5.2.a Obtain and review software development processes for any web-based payment applications (internal and external, and including web-administrative access to product). Verify the process includes training in secure coding techniques for developers, and is based on guidance such as the OWASP guide (http://www.owasp.org). Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques.</p> <p>5.2.b For web payment applications</p>	N/A. Sensible Cinema is not a web application.		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p><i>the OWASP guide is updated, the current version must be used for these requirements.</i></p> <p>PCI Data Security Standard Requirement 6.5</p>	<p>included in review, verify that the payment applications are not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing that specifically attempts to exploit each of the following:</p>	<p>application.</p>		
<p>5.2.1 Cross-site scripting (XSS).</p>	<p>5.2.1 Cross-site scripting (XSS) (Validate all parameters before inclusion.)</p>	<p>N/A. Sensible Cinema is not a web application.</p>		
<p>5.2.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws, as well as other injection flaws.</p>	<p>5.2.2 Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.)</p>	<p>N/A. Sensible Cinema is not a web application.</p>		
<p>5.2.3 Malicious file execution</p>	<p>5.2.3 Malicious file execution (Validate input to verify application does not accept filenames or files from users.)</p>	<p>N/A. Sensible Cinema is not a web application.</p>		
<p>5.2.4 Insecure direct object references.</p>	<p>5.2.4 Insecure direct object references (Do not expose internal object references to users.)</p>	<p>N/A. Sensible Cinema is not a web application.</p>		
<p>5.2.5 Cross-site request forgery (CSRF).</p>	<p>5.2.5 Cross-site request forgery (CSRF) (Do not rely on authorization credentials and tokens automatically submitted by browsers.)</p>	<p>N/A. Sensible Cinema is not a web application.</p>		
<p>5.2.6 Information leakage and improper error handling</p>	<p>5.2.6 Information leakage and improper error handling (Do not leak information via error messages or other means.)</p>	<p>N/A. Sensible Cinema is not a web application.</p>		
<p>5.2.7 Broken authentication and session management</p>	<p>5.2.7 Broken authentication and session management (Properly authenticate users and protect</p>	<p>N/A. Sensible Cinema is not a web application.</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	account credentials and session tokens.)			
5.2.8 Insecure cryptographic storage	5.2.8 Insecure cryptographic storage (Prevent cryptographic flaws.)	N/A. Sensible Cinema is not a web application.		
5.2.9 Insecure communications	5.2.9 Insecure communications (Properly encrypt all authenticated and sensitive communications.)	N/A. Sensible Cinema is not a web application.		
5.2.10 Failure to restrict URL access.	5.2.10 Failure to restrict URL access (Consistently enforce access control in presentation layer and business logic for all URLs.)	N/A. Sensible Cinema is not a web application.		
5.3 Software vendor must follow change control procedures for all product software configuration changes. The procedures must include the following: PCI Data Security Standard Requirement 6.4	5.3.a Obtain and examine the vendor's change-control procedures for software modifications, and verify that the procedures require items 5.3.1–5.3.4 below.			
	5.3.b Examine recent payment application changes, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures:			
5.3.1 Documentation of impact	5.3.1 Verify that documentation of customer impact is included in the change control documentation for each change.	403 Labs observed revision history and change management documents, reviewed the Software Development Procedures, and interviewed Rusty Gordon - Owner, who confirmed that they included customer impact.		
5.3.2 Management sign-off by appropriate parties	5.3.2 Verify that management sign-off by appropriate parties is present for each change.	N/A. Sensible Cinema is a single-person business and did not require management sign-off for changes.		
5.3.3 Testing of operational functionality	5.3.3 Verify that operational functionality testing was performed	403 Labs observed revision history and change management documents, reviewed the Software Development		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	for each change.	Procedures, and interviewed Rusty Gordon - Owner, who confirmed that they required operational functionality testing.		
5.3.4 Back-out or product de-installation procedures	5.3.4 Verify that back-out or product de-installation procedures are prepared for each change.	403 Labs observed revision history and change management documents, reviewed the Software Development Procedures, and interviewed Rusty Gordon - Owner, who confirmed that they included back-out procedures.		
5.4 The payment application must not use or require use of unnecessary and insecure services and protocols (for example, NetBIOS, file-sharing, Telnet, unencrypted FTP, etc.). PCI Data Security Standard Requirement 2.2.2	5.4 Examine system services, daemons, and protocols enabled or required by the payment application. Verify that unnecessary and insecure services or protocols are not enabled by default or required by the payment application (for example, FTP is not enabled, or is encrypted via SSH or other technology).	403 Labs observed application function and reviewed the system configuration settings, which showed that Sensible Cinema did not require unnecessary or insecure services, nor did it enable them by default.		
6. Protect wireless transmissions				
6.1 For payment applications using wireless technology, the wireless technology must be implemented securely. PCI Data Security Standard Requirements 1.2.3 & 2.1.1	6.1.a For payment applications developed by the vendor using wireless technology, and other wireless applications bundled with the payment application, verify that the wireless applications do not use vendor default settings and are configured in accordance with PCI Data Security Standard Requirement 2.1.1.	N/A. Sensible Cinema did not expressly make use of wireless technology.		
	6.1.b Examine the <i>PA-DSS Implementation Guide</i> , prepared by the vendor to verify that customers and resellers/integrators are instructed, if wireless is used, to install a firewall per PCI DSS Requirement 1.2.3.	403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema instructed customers to segment Sensible Cinema from wireless networks with a firewall. 403 Labs tested application function, which showed that it can operate with a firewall per the		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
		<p>recommendation.</p> <p>Sensible Cinema did not make use of resellers or integrators.</p>		
<p>6.2 For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.</p> <p>Payment applications using wireless technology must facilitate the following regarding use of WEP:</p> <ul style="list-style-type: none"> ▪ <i>For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.</i> ▪ <i>For current wireless implementations, it is prohibited to use WEP after June 30, 2010.</i> <p>PCI Data Security Standard Requirement 4.1.1</p>	<p>6.2.a For payment applications developed by the vendor using wireless technology, and other wireless applications bundled with the vendor application, verify that industry best practices (for example, IEEE 802.11.i) were used to include or make available strong encryption for authentication and transmission, in accordance with PCI DSS Requirement 4.1.1.</p> <p>6.2.b If customers could implement the payment application into a wireless environment, examine <i>PA-DSS Implementation Guide</i> prepared by vendor to verify customers and resellers/integrators are instructed on PCI DSS-compliant wireless settings, per PCI DSS Requirements 1.2.3, 2.1.1 and 4.1.1.</p>	<p>N/A. Sensible Cinema did not expressly make use of wireless technology.</p> <p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema instructed customers to implement wireless networks securely, specifically:</p> <ul style="list-style-type: none"> ▪ Implement a firewall between Sensible Cinema and wireless networks and document and control or deny any access between the wireless network and Sensible Cinema. ▪ Change default settings on wireless networks, specifically: <ul style="list-style-type: none"> ○ Default encryption keys ○ Default SNMP community strings ○ Default passwords for access points ○ Update firmware to support strong encryption for authentication and data 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
		transmission <ul style="list-style-type: none"> ○ Enable WPA or WPA2, if supported ○ Other values from wireless access points as needed <ul style="list-style-type: none"> ▪ Use industry best practices to implement strong encryption for authentication and transmission. Sensible Cinema did not make use of resellers or integrators.		
7. Test payment applications to address vulnerabilities				
<p>7.1 Software vendors must establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet) and to test their payment applications for vulnerabilities. Any underlying software or systems that are provided with or required by the payment application (for example, web servers, 3rd-party libraries and programs) must be included in this process.</p> <p>PCI Data Security Standard Requirement 6.2</p>	<p>7.1.a Obtain and examine processes to identify new vulnerabilities and to test payment applications for new vulnerabilities. Verify the processes include:</p> <ul style="list-style-type: none"> ▪ Using outside sources for security vulnerability information ▪ Testing of payment applications for new vulnerabilities <p>7.1.b Verify that processes to identify new vulnerabilities and implement corrections into payment application apply to all software provided with or required by the payment application (for example, web servers, third-party libraries and programs).</p>	<p>403 Labs observed revision history and change management documents and reviewed the Software Development Procedures, which showed that Sensible Cinema adhered to the following process:</p> <ul style="list-style-type: none"> ▪ Obtained information about new vulnerabilities from outside sources ▪ Tested Sensible Cinema for new vulnerabilities. <p>403 Labs observed revision history and change management documents and reviewed the Software Development Procedures, which showed that Sensible Cinema's vulnerability management process included information about components and libraries used.</p>		
<p>7.2 Software vendors must establish a process for timely development and deployment of security patches and upgrades, which includes delivery of</p>	<p>7.2.a Obtain and examine processes to develop and deploy security patches and upgrades for software. Verify the processes include:</p>	<p>403 Labs observed revision history and change management documents and reviewed the Software Development Procedures, which</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p>updates and patches in a secure manner with a known chain-of-trust, and maintenance of the integrity of patch and update code during delivery and deployment.</p>	<ul style="list-style-type: none"> ▪ Timely development and deployment of patches to customers ▪ Delivery of patches and updates in a secure manner with a known chain-of-trust ▪ Delivery of patches and updates in a manner that maintains the integrity of the deliverable ▪ Integrity testing of the patch or update by the target system prior to installation 	<p>showed that Sensible Cinema:</p> <ul style="list-style-type: none"> ▪ Provided timely updates and delivery of patches to customers ▪ Required customers to obtain patches directly from Sensible Cinema ▪ Allowed for delivery that maintained integrity of the deliverable ▪ Allowed for integrity testing of the patch prior to installation 		
	<p>7.2.b To verify that the integrity of patch and update code is maintained, run the update process with arbitrary code and determine that the system will not allow the update to occur.</p>	<p>403 Labs observed application function, which showed that updates can only be run with Sensible Cinema-supplied update code and did not execute with arbitrary code.</p>		
<p>8. Facilitate secure network implementation</p>				
<p>8.1 The payment application must be able to be implemented into a secure network environment. Application must not interfere with use of devices, applications, or configurations required for PCI DSS compliance (for example, payment application cannot interfere with anti-virus protection, firewall configurations, or any other device, application, or configuration required for PCI DSS compliance).</p> <p><i>PCI Data Security Standard Requirements 1, 3, 4, 5, and 6.6</i></p>	<p>8.1 Test the payment application in a lab to obtain evidence that it can run in a network that is fully compliant with PCI DSS. Verify that the payment application does not inhibit installation of patches or updates to other components in the environment.</p>	<p>403 Labs observed application function and reviewed the system configuration settings, which showed that Sensible Cinema did not inhibit installation of patches or updates to other components in the environment.</p>		
<p>9. Cardholder data must never be stored on a server connected to the Internet</p>				
<p>9.1 The payment application must be developed such that the database server and web server are not required to be on the same server, nor</p>	<p>9.1.a To verify that the payment application stores cardholder data in the internal network, and never in the DMZ, obtain evidence that the</p>	<p>403 Labs observed application function, reviewed system configuration settings, and reviewed the PA-DSS Implementation Guide,</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
<p>is the database server required to be in the DMZ with the web server.</p> <p>PCI Data Security Standard Requirement 1.3.2</p>	<p>payment application does not require data storage in the DMZ, and will allow use of a DMZ to separate the Internet from systems storing cardholder data (for example, payment application must not require that the database server and web server be on the same server, or in the DMZ with the web server).</p>	<p>which did not show evidence it required direct, inbound Internet access, nor did it require data storage in a DMZ.</p>		
	<p>9.1.b If customers could store cardholder data on a server connected to the Internet, examine <i>PA-DSS Implementation Guide</i> prepared by vendor to verify customers and resellers/integrators are told not to store cardholder data on Internet-accessible systems (for example, web server and database server must not be on same server).</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema instructed customers not to place Sensible Cinema in a DMZ.</p> <p>Sensible Cinema did not use resellers or integrators.</p>		

10. Facilitate secure remote software updates

<p>10.1 If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure "always-on" connections.</p> <p>PCI Data Security Standard Requirements 1 and 12.3.9</p>	<p>10.1 If the vendor delivers payment application and/or updates via remote access to customer networks, examine <i>PA-DSS Implementation Guide</i> prepared by vendor, and verify it contains:</p> <ul style="list-style-type: none"> ▪ Instructions for customers and resellers/integrators regarding secure use of remote-access technologies, per PCI DSS Requirement 12.3.9 ▪ Recommendation for customers and resellers/ integrators to use a firewall or a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these "always-on" connections, per PCI DSS Requirement 1 	<p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema did not require remote access for software updates.</p>		
--	---	---	--	--

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
11. Facilitate secure remote access to payment application				
<p>11.1 The payment application must not interfere with use of a two-factor authentication mechanism. The payment application must allow for technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates.</p> <p>PCI Data Security Standard Requirement 8.3</p>	<p>11.1 Test the payment application in a lab to obtain evidence that it can run with a two-factor authentication mechanism (the payment application must not prohibit an organization's ability to implement two-factor authentication).</p>	<p>403 Labs observed application function and reviewed the system configuration settings, which showed that Sensible Cinema could operate in conjunction with two-factor authentication for remote access.</p>		
<p>11.2 If the payment application may be accessed remotely, remote access to the payment application must be authenticated using a two-factor authentication mechanism.</p> <p>PCI Data Security Standard Requirement 8.3</p>	<p>11.2 If the payment application may be accessed remotely, examine <i>PA-DSS Implementation Guide</i> prepared by the software vendor, and verify it contains instructions for customers and resellers/integrators regarding required use of two-factor authentication (user ID and password and an additional authentication item such as a smart card, token, or PIN).</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema advised customers to implement secure remote access with two-factor authentication.</p> <p>Sensible Cinema did not use resellers or integrators.</p>		
<p>11.3 If vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely.</p> <p>PCI Data Security Standard Requirement 8.3</p>	<p>11.3.a If the software vendor uses remote access products for remote access to the customers' payment application, verify that vendor personnel implement and use remote access security features.</p> <p><i>Note: Examples of remote access security features include:</i></p> <ul style="list-style-type: none"> ▪ <i>Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).</i> ▪ <i>Allow connections only from specific (known) IP/MAC addresses.</i> ▪ <i>Use strong authentication and</i> 	<p>N/A. Sensible Cinema did not use remote access products to connect to customer installations.</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	<p><i>complex passwords for logins according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15</i></p> <ul style="list-style-type: none"> ▪ <i>Enable encrypted data transmission according to PCI DSS Requirement 4.1</i> ▪ <i>Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13</i> ▪ <i>Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed.</i> ▪ <i>Enable the logging function.</i> ▪ <i>Restrict access to customer passwords to authorized reseller/integrator personnel.</i> ▪ <i>Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.</i> 			
	<p>11.3.b If resellers/integrators or customers can use remote access software, examine <i>PA-DSS Implementation Guide</i> prepared by the software vendor, and verify that customers and resellers/integrators are instructed to use and implement remote access security features.</p> <p><i>Note: Examples of remote access security features include:</i></p> <ul style="list-style-type: none"> ▪ <i>Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).</i> 	<p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema instructed customers to implement appropriate remote access security features, specifically:</p> <ul style="list-style-type: none"> ▪ Changing default settings and passwords. ▪ Restricting connections to known IP or MAC addresses. ▪ Use strong authentication and complex passwords, specifically: <ul style="list-style-type: none"> ○ Require unique usernames for all users. 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	<ul style="list-style-type: none"> ▪ <i>Allow connections only from specific (known) IP/MAC addresses.</i> ▪ <i>Use strong authentication and complex passwords for logins, according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15.</i> ▪ <i>Enable encrypted data transmission according to PCI DSS Requirement 4.1.</i> ▪ <i>Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13.</i> ▪ <i>Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed.</i> ▪ <i>Enable the logging function.</i> ▪ <i>Restrict access to customer passwords to authorized reseller/integrator personnel.</i> ▪ <i>Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.</i> 	<ul style="list-style-type: none"> ○ Required passwords for authentication ○ Required two-factor authentication for remote access ○ Prohibited the use of shared, generic, or group user accounts or passwords ○ Required password changes every 90 days ○ Required passwords of at least seven characters in length ○ Required alphanumeric passwords ○ Prevented the reuse of the prior four passwords ○ Locked out accounts after six invalid login attempts ○ Required account lockout for 30 minutes ○ Time out after 15 minutes of inactivity ▪ Enable encrypted data transmission using strong encryption. ▪ Configure systems to require a VPN for remote access. ▪ Enable logging and reviewing logs regularly. ▪ Restricting access to customer passwords to only authorized reseller personnel -N/A. Sensible Cinema did not use resellers. ▪ Establishing customer 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
		passwords, according to the following: <ul style="list-style-type: none"> ○ Require unique usernames for all users. ○ Require password authentication for all users. ○ Require password encryption for passwords in storage and transmission. ○ Prohibited the use of shared, generic, or group user accounts or passwords ○ Required password changes every 90 days ○ Require passwords of at least seven characters in length ○ Required alphanumeric passwords ○ Prevented the reuse of the prior four passwords ○ Locked out accounts after six invalid login attempts ○ Required account lockout for 30 minutes ○ Time out after 15 minutes of inactivity 		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
12. Encrypt sensitive traffic over public networks				
<p>12.1 If the payment application sends, or facilitates sending, cardholder data over public networks, the payment application must support use of strong cryptography and security protocols such as SSL/TLS and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p><i>Examples of open, public networks that are in scope of the PCI DSS are:</i></p> <ul style="list-style-type: none"> ▪ <i>The Internet</i> ▪ <i>Wireless technologies</i> ▪ <i>Global System for Mobile Communications (GSM)</i> ▪ <i>General Packet Radio Service (GPRS)</i> <p>PCI Data Security Standard Requirement 4.1</p>	<p>12.1.a If the payment application sends, or facilitates sending, cardholder data over public networks, verify that secure encryption transmission technology (for example, IPSEC, VPN or SSL/TLS) is provided, or that use thereof is specified.</p> <p>12.1.b If the payment application allows data transmission over public networks, examine <i>PA-DSS Implementation Guide</i> prepared by the vendor, and verify the vendor includes directions for customers and resellers/integrators to use secure encryption transmission technology (for example, IPSEC, VPN or SSL/TLS).</p>	<p>403 Labs observed a sample of four transactions and reviewed the Software Development Procedures, which showed that Sensible Cinema communicated over HTTPS when performing transactions over public networks.</p> <p>403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema required HTTPS for transactions and that these settings were not configurable.</p>		
<p>12.2 The payment application must never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).</p> <p>PCI Data Security Standard Requirement 4.2</p>	<p>12.2.a If the payment application allows and/or facilitates sending of PANs by end-user messaging technologies, verify that a strong cryptography solution is provided, or that use thereof is specified.</p> <p>12.2.b If the payment application allows and/or facilitates the sending of PANs by end-user messaging technologies, examine <i>PA-DSS Implementation Guide</i> prepared by the vendor, and verify the vendor includes directions for customers and resellers/integrators to use a solution that implements strong cryptography.</p>	<p>N/A. Sensible Cinema did not support the use of end-user messaging technologies for sending cardholder data.</p> <p>N/A. Sensible Cinema did not support the use of end-user messaging technologies for sending cardholder data.</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
13. Encrypt all non-console administrative access				
<p>13.1 Instruct customers to encrypt all non-console administrative access using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</p> <p>PCI Data Security Standard Requirement 2.3</p> <p><i>Telnet or rlogin must never be used for administrative access.</i></p>	<p>13.1 If payment application or server allows non-console administration, examine the <i>PA-DSS Implementation Guide</i> prepared by vendor, and verify vendor recommends use of SSH, VPN, or SSL/TLS for encryption of non-console administrative access.</p>	<p>N/A. 403 Labs reviewed the PA-DSS Implementation Guide, which showed that Sensible Cinema did not facilitate non-console administrative access.</p>		
14. Maintain instructional documentation and training programs for customers, resellers, and integrators				
<p>14.1 Develop, maintain, and disseminate a <i>PA-DSS Implementation Guide(s)</i> for customers, resellers, and integrators that accomplishes the following:</p>	<p>14.1 Examine the <i>PA-DSS Implementation Guide</i> and related processes, and verify the guide is disseminated to all relevant payment application users (including customers, resellers, and integrators).</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide and observed distribution process, which showed that Sensible Cinema distributed the PA-DSS Implementation Guide to all customers. Sensible Cinema did not make use of resellers or integrators.</p>		
<p>14.1.1 Addresses all requirements in this document wherever the <i>PA-DSS Implementation Guide</i> is referenced.</p>	<p>14.1.1 Verify the <i>PA-DSS Implementation Guide</i> covers all related requirements in this document.</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide and observed update markings in the document, which showed that the guide covered all requirements in the PA-DSS.</p>		
<p>14.1.2 Includes a review at least annually and updates to keep the documentation current with all major and minor software changes as well as with changes to the requirements in this document.</p>	<p>14.1.2.a Verify the <i>PA-DSS Implementation Guide</i> is reviewed on an annual basis and updated as needed to document all major and minor changes to the payment application.</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide and observed update markings in the document, which showed that Sensible Cinema had a process to revise and update the guide on at least an annual basis or when major changes occur with the application.</p>		
	<p>14.1.2.b Verify the <i>PA-DSS Implementation Guide</i> is reviewed on an annual basis and updated as</p>	<p>403 Labs reviewed the PA-DSS Implementation Guide and observed update markings in the document,</p>		

PA-DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date / Comments
	needed to document changes to the PA-DSS requirements.	which showed that Sensible Cinema had a process to revise and update the guide when updates are made to the PA-DSS.		
14.2 Develop and implement training and communication programs to ensure payment application resellers and integrators know how to implement the payment application and related systems and networks according to the <i>PA-DSS Implementation Guide</i> and in a PCI DSS-compliant manner.	14.2 Examine the training materials and communication program for resellers and integrators, and confirm the materials cover all items noted for the <i>PA-DSS Implementation Guide</i> throughout this document.	N/A. Sensible Cinema did not use resellers or integrators.		
14.2.1 Update the training materials on an annual basis and whenever new payment application versions are released.	14.2.1.a Examine the training materials for resellers and integrators and verify the materials are reviewed on an annual basis and when new payment application versions are released, and updated as needed.	N/A. Sensible Cinema did not use resellers or integrators.		
	14.2.1.b Examine the distribution process for new payment application versions and verify that updated documentation is distributed with the updated payment application.	N/A. Sensible Cinema did not use resellers or integrators.		
	14.2.1.c Select a sample of resellers and integrators and interview them to verify they received the training materials.	N/A. Sensible Cinema did not use resellers or integrators.		

Appendix B: Confirmation of Testing Laboratory Configuration Specific to PA-DSS Assessment

For: *Sensible Cinema 2009*

For each PA-DSS assessment conducted, the PA-QSA must complete this document to confirm the status and capabilities of the laboratory used to conduct the testing for the PA-DSS assessment. This completed document must be submitted along with the completed PA-DSS Requirements and Security Assessment Procedures document.

For each Laboratory Validation Procedures, indicate (by using columns titled “Completed in PA-QSA’s Lab” or “Completed in Vendor’s Lab”) whether laboratory used for the assessment and the laboratory undergoing these Validation Procedures was the PA-QSA’s laboratory or software vendor’s laboratory.

Describe laboratory testing architecture and environment in place for this PA-DSS review: 403 Labs tested Sensible Cinema on a Windows XP machine with current security patches and ClamWin anti-virus software on a network segment with a Fortigate firewall.

Describe how the real-world use of the payment application was simulated in the laboratory for this PA-DSS review: 403 Labs tested transactions using test cards from the payment processor to show application function, data flows, and security functions.

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA’s Lab	Completed in Vendor’s Lab	Comments
1. <i>Install payment application per vendor’s installation instructions or training provided to customer.</i>	1. Verify that the vendor’s installation manual or training provided to customers was used to perform the default installation for the payment application product on all platforms listed in the PA-DSS report.	403 Labs used the Sensible Cinema installation instructions to perform the default installation.		

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
2. Install and test all payment application versions listed in PA-DSS report.	2.a Verify that all common implementations (including region/country specific versions) of the payment application to be tested were installed.	403 Labs tested all common implementation of the application.		
	2.b Verify that all payment application versions and platforms were tested.	403 Labs tested the only version being assessed.		
	2.c Verify that all critical payment application functionalities were tested.	403 Labs tested all critical payment application functionalities.		
3. Install and implement all PCI DSS required security devices.	3. Verify that all security devices required by PCI DSS (for example, firewalls and anti-virus software) were implemented on test systems.	403 Labs tested the application in conjunction with all necessary security devices.		
4. Install and/or configure all PCI DSS required security settings.	4. Verify all PCI DSS-compliant system settings, patches, etc. were implemented on test systems for operating systems, system software, and applications used by the payment application.	403 Labs tested the application in conjunction with all PCI DSS-compliant system settings, patches, etc.		

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
<p>5. Simulate real-world use of the payment application.</p>	<p>5.a The laboratory simulates the 'real world' use of the payment application, including all systems and applications where the payment application is implemented. For example, a standard implementation of a payment application might include a client/server environment within a retail storefront with a POS machine, and back office or corporate network. The laboratory simulates the total implementation.</p>	<p>403 Labs simulated a real world use of the payment application for testing.</p>		
<p>5.b The laboratory uses only test card numbers for the simulation/testing—live PANs are not used for testing.</p> <p><i>Note: Test cards can usually be obtained from the vendor or a processor or acquirer.</i></p>		<p>403 Labs tested the application with only test cards.</p>		
	<p>5.c The laboratory runs the payment application's authorization and/or settlement functions and all output is examined per item 6 below.</p>	<p>403 Labs tested the application's authorization and settlement functions and examined all output.</p>		
	<p>5.d The laboratory and/or processes map all output produced by the payment application for every possible scenario, whether temporary, permanent, error processing, debugging mode, log files, etc.</p>	<p>403 Labs tested the application such that it mapped out all output for each scenario, including errors, etc.</p>		

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
	<p>5.e The laboratory and/or processes simulate and validate all functions of the payment application, to include generation of all error conditions and log entries using both simulated 'live' data and invalid data.</p>	<p>403 Labs tested all functions of the payment application for error conditions using both valid and invalid data.</p>		
<p>6. Provide capabilities for, and test using, the following penetration testing methodologies:</p>	<p>6.a Use of forensic tools/methods⁶: Forensic tools/methods were used to search all identified output for evidence of sensitive authentication data (commercial tools, scripts, etc.), per PA-DSS Requirement 1.1.1–1.1.3.³</p>	<p>403 Labs used forensic tools and methods to search for sensitive authentication data.</p>		
	<p>6.b Attempt to exploit QWASP vulnerabilities: OWASP vulnerabilities were used to attempt to exploit the payment application(s), per PA-DSS Requirement 5.1.1–5.1.10.</p>			<p>N/A. Sensible Cinema was not a web application.</p>
	<p>6.c Laboratory and/or processes attempted to execute arbitrary code during the payment application update process: Run the update process with arbitrary code per PA-DSS requirement 7.2.b.</p>	<p>403 Labs attempted to execute arbitrary code during the application update process.</p>		

³ Forensic tool or method: A tool or method for uncovering, analyzing and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly. In the case of forensic tools or methods used by PA-QSAs, these tools or methods should accurately locate any sensitive authentication data written by the payment application. These tools may be commercial, open-source, or developed in-house by the PA-QSA.

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
7. Use vendor's lab ONLY after verifying all requirements are met.	7.a If use of the software vendor's lab is necessary (for example, the PA-QSA does not have the mainframe, AS400, or Tandem the payment application runs on), the PA-QSA can either (1) use equipment on loan from the Vendor or (2) use the vendor's lab facilities, provided that this is detailed in the report together with the location of the tests. For either option, the PA-QSA verified that the vendor's equipment and lab meet the following requirements:			N/A. The vendor's laboratory was not used.
	7.b The PA-QSA verifies that the vendor's lab meets all above requirements specified in this document and documents the details in the report.			N/A. The vendor's laboratory was not used.
	7.c All testing is executed by the PA-QSA (the vendor cannot run tests against their own application).			N/A. The vendor's laboratory was not used.
	7.d All testing is either (1) performed while on-site at the vendor's premises, or (2) performed remotely via a network connection using a secure link (for example, VPN).			N/A. The vendor's laboratory was not used.
	7.e Use only test card numbers for the simulation/testing—do not use live PANs for testing. These test cards can usually be obtained from the vendor or a processor or acquirer.			N/A. The vendor's laboratory was not used.
8. Maintain an effective quality assurance (QA) process	8.a PA-QSA QA personnel verifies that all platforms identified in the PA-DSS report were included in testing.	403 Labs QA verified that all platforms were included in testing.		
	8.b PA-QSA QA personnel verify that all PA-DSS requirements were tested against.	403 Labs QA verified that all requirements were tested.		

Laboratory Requirement	Laboratory Validation Procedure	Completed in PA-QSA's Lab	Completed in Vendor's Lab	Comments
	8.c The PA-QSA QA personnel verify that PA-QSA laboratory configurations and processes meet requirements and were accurately documented in the report.	403 Labs QA verified that the laboratory configuration met the requirements and were documented accurately.		
	8.d PA-QSA QA personnel verify that the report accurately presents the results of testing.	403 Labs QA verified that the report accurately represents the testing results.		

Appendix C: Attestation of Validation

Instructions for Submission

The Payment Application Qualified Security Assessor (PA-QSA) must complete this document as a declaration of the payment application's validation status with the Payment Application Data Security Standard (PA-DSS). Complete all applicable sections of this Attestation of Validation. Submit the PA-DSS Report on Validation (ROV), this attestation, and the completed PA-DSS Appendix B to PCI SSC. Once accepted by PCI SSC, the payment application will be posted on the PCI SSC website as a PA-DSS validated payment application.

The PA-QSA and Payment Application Software Vendor should complete all sections and submit this document along with copies of all required validation documentation to PCI SSC, per PCI SSC's instructions for report encryption and submission.

Part 1. Payment Application Qualified Security Assessor (PA QSA) Company Information

<i>Company Name:</i>	403 Labs, LLC		
<i>Lead PA-QSA Contact Name:</i>	Jacob Ansari	<i>Title:</i>	Manager – Technical Services
<i>Telephone:</i>	877.403.5227 x215	<i>E-mail:</i>	jansari@403labs.com
<i>Business Address:</i>	17125C W Bluemound Road Suite 100	<i>City:</i>	Brookfield
<i>State/Province:</i>	WI	<i>Country:</i>	USA
		<i>ZIP:</i>	53005
<i>URL:</i>	www.403labs.com		

Part 2. Payment Application Vendor Information

<i>Company Name:</i>	Sensible Cinema Software		
<i>Contact Name:</i>	Rusty Gordon	<i>Title:</i>	Owner
<i>Telephone:</i>	615.799.6367	<i>E-mail:</i>	info@sensiblecinema.com
<i>Business Address:</i>	7216 Sutton Pl	<i>City:</i>	Fairview
<i>State/Province:</i>	TN	<i>Country:</i>	USA
		<i>ZIP:</i>	37062
<i>URL:</i>	www.sensiblecinema.com		

Part 2a. Payment Application Information

List Payment Application Name(s) and Version Number(s) included in PA-DSS review: Sensible Cinema 2009

Payment Application Functionality (check all that apply):

- | | | |
|---|---|---|
| <input checked="" type="checkbox"/> Point of Sale | <input type="checkbox"/> Shopping Cart | <input type="checkbox"/> Card-not-present |
| <input type="checkbox"/> Middleware | <input type="checkbox"/> Settlement | <input type="checkbox"/> Gateway |
| <input type="checkbox"/> Automated Fuel Dispenser | <input type="checkbox"/> Others (please specify): | |

Target Market for Application: Cinemas

Part 3. PCI PA-DSS Validation

Part 3a. Confirmation of Validated Status

Based on the results noted in the PA-DSS ROV dated *July 3, 2009*, *403 Labs, LLC* asserts the following validation status for the application(s) and version(s) identified in Part 2a of this document as of *July 3, 2009* (check one):

<input checked="" type="checkbox"/>	Fully Validated: All requirements in the ROV are marked “in place,” thereby <i>Sensible Cinema 2009</i> has achieved full validation with the Payment Application Data Security Standard.
<input checked="" type="checkbox"/>	The ROV was completed according to the PA-DSS, version <i>1.2</i> , in adherence with the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROV and in this attestation represents the results of the assessment fairly in all material respects.
<input checked="" type="checkbox"/>	No evidence of magnetic stripe (i.e., track) data ⁴ , CAV2, CVC2, CID, or CVV2 data ⁵ , or PIN data ⁶ storage after transaction authorization on ANY files or functionalities generated by the application during this PA-DSS assessment.

Part 3b. Annual Re-Validation Confirmation:

The contents of the above-referenced ROV continue to be applicable to the following software version: (*Payment Application Name and version*).

Note: Section 3b is for the required Annual Attestation for listed payment applications, and should ONLY be completed if no modifications have been made to the Payment Application covered by the above-referenced ROV.

Part 3c. PA-QSA and Application Vendor Acknowledgments

<i>Signature of Lead PA-QSA</i> ↑	<i>Date</i> ↑
Jacob Ansari	Manager, Technical Services
<i>Lead PA-QSA Name</i> ↑	<i>Title</i> ↑
<i>Signature of Application Vendor Executive Officer</i> ↑	<i>Date</i> ↑
Rusty Gordon	Owner
<i>Application Vendor Executive Officer Name</i> ↑	<i>Title</i> ↑
Sensible Cinema Software	
<i>Application Vendor Company Represented</i> ↑	

⁴ Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after authorization. The only elements of track data that may be retained are account number, expiration date, and name.

⁵ The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

⁶ PIN Data – Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.