



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 1

Publication Date: December 2022



PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

**Entity Name: Passage HoldCo, LLC
Mobile Acept North America, Inc.
Monetra Technologies, LLC
Pace Payment Systems, Inc.
Pace Payments, Inc.**

Assessment End Date: August 30, 2024

Date of Report as noted in the Report on Compliance: August 30, 2024



Section 1 Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider’s assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* (“Assessment”). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	Passage HoldCo, LLC Mobile Acept North America, Inc. Monetra Technologies, LLC Pace Payment Systems, Inc. Pace Payments, Inc.
DBA (doing business as):	Monetra, TranSafe, Pace, PlacePay, mobileAcept, Bill and Pay, Fairway Payments
Company mailing address:	40 Burton Hills Blvd., Ste 415, Nashville, TN 37215
Company main website:	https://www.i3verticals.com/
Company contact name:	Paul Maple
Company contact title:	i3 Verticals General Counsel & Corporate Secretary
Contact phone number:	615-465-4487
Contact e-mail address:	pmaple@i3verticals.com

Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)

ISA name(s):	Not Applicable
--------------	-----------------------

Qualified Security Assessor

Company name:	Frazier & Deeter, LLC
Company mailing address:	1230 Peachtree Street NE Suite 1500 Atlanta, GA 30309
Company website:	https://www.frazierdeeter.com/
Lead Assessor name:	Jessie Sandell
Assessor phone number:	615-416-6882



Assessor e-mail address:	jessie.sandell@frazierdeeter.com
Assessor certificate number:	QSA 206-329

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were **INCLUDED** in the scope of the Assessment (select all that apply):

Name of service(s) assessed: Bill and Pay, BIS, Burton (including Velocity), CourtSolutions ("CS") and EZCourtPay ("EZCP"), i3 Education (including SchoolPay, PaySchools, EZPay, and Local Level), iGov Solutions, mobileAxept, Pace PlacePay TranSafe (including Monetra)

Type of service(s) assessed:

Hosting Provider:

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web-hosting services
- Security services
- 3-D Secure Hosting Provider
- Multi-Tenant Service Provider
- Other Hosting (specify):

Managed Services:

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

Payment Processing:

- POI / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- Other processing (specify):

- | | | |
|--|---|--|
| <input type="checkbox"/> Account Management | <input type="checkbox"/> Fraud and Chargeback | <input checked="" type="checkbox"/> Payment Gateway/Switch |
| <input checked="" type="checkbox"/> Back-Office Services | <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Prepaid Services |
| <input checked="" type="checkbox"/> Billing Management | <input type="checkbox"/> Loyalty Programs | <input type="checkbox"/> Records Management |
| <input type="checkbox"/> Clearing and Settlement | <input checked="" type="checkbox"/> Merchant Services | <input type="checkbox"/> Tax/Government Payments |

Network Provider

Others (specify):

Note: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.



Part 2a. Scope Verification (continued)

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Retail POS, Merchant Services and anything else not explicitly stated above
----------------------------------	---

Type of service(s) not assessed:

Hosting Provider:	Managed Services:	Payment Processing:
<input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<input checked="" type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input checked="" type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input checked="" type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

Provide a brief explanation why any checked services were not included in the Assessment:	Services provided by the service provider that were not included in this assessment were either not material to the service provider's business, did not store, process, transmit, or otherwise impact the security of CHD, or were covered in another compliance assessment and therefore excluded from this DSS assessment. The services offered by the provider are re-evaluated annually to determine whether they should be included in a DSS or other compliance assessment.
---	--

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	mobileAxept Payment data received by mobileAxept are transmitted for processing via HTTPS over port 443 secured with
---	---



	<p>TLS v1.2. A unique transaction token and the last four digits of the card number are retained in the mobileAxept database.</p> <p>Bill & Pay Payment data received by Bill and Pay are transmitted for processing via HTTPS over port 443 secured with TLS v1.2. A unique transaction token and the last four digits of the card number are retained in the Bill and Pay database.</p> <p>PlacePay Payment data received by PlacePay are transmitted for processing via HTTPS over port 443 secured with TLS v1.2. Account data persists in the PlacePay database and secured via strong cryptography.</p> <p>Fuze Payment data received by the Fuze APIs are transmitted to TranSafe via HTTPS over port 443 secured with TLS v1.2. Fuze retains only tokens in its database.</p> <p>TranSafe (including Monetra) Payment data received by TranSafe are transmitted to the appropriate processor over port 443 secured with TLS v1.2. Account data persists in the TranSafe database and secured via strong cryptography.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>Passage HoldCo is responsible for securing account data at all stages of the transaction lifecycle--including its reception via in-person or ecommerce payment channels, its transit over the Internet, and any storage when secured rest within any Passage HoldCo database. As a third-party service provider, Passage HoldCo is aware of its ability to impact the security of its customers' account data and has taken care to implement the necessary controls required achieve and maintain security compliance.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>Passage HoldCo technologies that could impact the security of account data include AWS infrastructure-as-a-service (IaaS) products (e.g., EC2, Network Security Groups, and GuardDuty) network security controls at i3 Private Cloud datacenters (e.g., Juniper firewalls), endpoint protection technologies (e.g., Defender for Endpoint and TrendMicro) WAF technologies (e.g., Cloudflare, AWS WAF, ModSecurity), database technologies such as MariaDB; administrator workstations (including laptops); and authentication services such as JumpCloud.</p>



Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment.

For example:

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

mobileAxept
mobileAxept tokenizes cardholder data, enabling donors to make recurring or one-time donations to organizations. Donors create a profile with their demographic and payment information, allowing them to make ongoing donations to their chosen organization without needing to re-enter their card information after the initial setup.

Bill & Pay
Bill & Pay is an invoicing and billing platform that helps businesses to manage their payment and account receivables processes. It serves as a central solution for businesses to create and track invoices and for customers to receive and pay bills.

PlacePay
PlacePay is a payment solution designed for the real estate industry, handling property management transactions such as homeowners' association (HOA) fees, rent payments, and commercial real estate payments

Pace Payments
Pace Payments is a provider of fully integrated payment and transaction solutions tailored to the public sector and education industry. Pace markets, distributes, and sells payment processing products, including software, primarily through integrated partnerships within these verticals. One of the Fuze implementations ("Fuze 1.0" is offered and managed by Atlantic-Pacific Processing Systems (APPS).

TranSafe (including Monetra)
Monetra is a PCI-SSF validated application purpose-built to scale from small custom embedded devices to fully redundant payment servers capable of processing thousands of transactions per minute. TranSafe is the SaaS form of the Monetra gateway where Passage HoldCo hosts and manages the underlying infrastructure of the solution, including the storage and processing of transaction and account data.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

Yes No



(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)

**Part 2d. In-Scope Locations/Facilities
(ROC Section 4.6)**

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Datacenters (AWS)	619	(Refer to AWS PCI DSS AOC)
Datacenters (i3 Private Cloud)	3	Jacksonville, FL Atlanta, GA Charlotte, NC



**Part 2e. PCI SSC Validated Products and Solutions
(ROC Section 3.3)**

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

Yes No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Monetra	9.x.y	Secure Software Standard v1.1	22-45.01232.001	1 Oct 2025

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions).



**Part 2f. Third-Party Service Providers
(ROC Section 4.4)**

For the services being validated, does the entity have relationships with one or more third-party service providers that:

- | | |
|--|---|
| <ul style="list-style-type: none"> • Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <ul style="list-style-type: none"> • Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <ul style="list-style-type: none"> • Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services (AWS)	Infrastructure hosting
TSYS / Global Payments	Payment processing
Cloudflare	WAF/DNS
Worldpay	Payment Processing
Cologix, Inc.	Third party data center
Digital Realty Trust, L.P.	Third party data center
EVOPLS, Inc	Third party data center
Paymentech, LLC	Payment Processing
Elavon North America	Payment Processing
First Data Merchant Services	Payment Processing
i3 Payfac (Burton/Velocity)	Payment Processing

Note: Requirement 12.8 applies to all entities in this list.



**Part 2g. Summary of Assessment
(ROC Section 1.8.1)**

Indicate below all responses provided within each principal PCI DSS requirement.

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3.2)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>		April 22, 2024
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>		August 30, 2024
Were any requirements in the ROC unable to be met due to a legal constraint?		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Examine documentation	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Interview personnel	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Examine/observe live data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe process being performed	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe physical environment	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
• Interactive testing	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Other: N/A	<input type="checkbox"/> Yes	<input type="checkbox"/> No



Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated August 30, 2024

Indicate below whether a full or partial PCI DSS assessment was completed:

- Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.
- Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (*select one*):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT rating; thereby Passage HoldCo, LLC Mobile Asept North America, Inc. Monetra Technologies, LLC Pace Payment Systems, Inc. Pace Payments, Inc. has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>				
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating; thereby (<i>Service Provider Company Name</i>) has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance:</p> <p>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.</p>				
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby (<i>Service Provider Company Name</i>) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="width: 30%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td style="height: 40px;"></td> <td></td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met		
Affected Requirement	Details of how legal constraint prevents requirement from being met				




Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

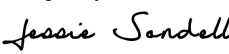
<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.


Part 3b. Service Provider Attestation

Signed by: 	
<small>428B706093EA432...</small> Signature of Service Provider Executive Officer ↑	Date: September 4, 2024 5:27 PM EDT
Service Provider Executive Officer Name: Paul Maple	Title: General Counsel & Secretary

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance.
If selected, describe all role(s) performed: Not Applicable	

Signed by: 	
<small>E19053C855614F1...</small> Signature of Lead QSA ↑	Date: September 4, 2024
Lead QSA Name: Jessie Sandell	

DocuSigned by: 	
<small>B67FB0EG6BC2444...</small> Signature of Duly Authorized Officer of QSA Company ↑	Date: September 4, 2024
Duly Authorized Officer Name: Mindy Milliet	QSA Company: Frazier & Deeter, LLC

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> ISA(s) provided other assistance.
If selected, describe all role(s) performed: Not Applicable	



Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

