



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.2.1**

June 2018



## Section 1: Assessment Information

### ***Instructions for Submission***

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

### **Part 1. Service Provider and Qualified Security Assessor Information**

#### **Part 1a. Service Provider Organization Information**

Company Name:	Systems East, Inc.		DBA (doing business as):	
Contact Name:	Peter Rogati		Title:	Director of Operations
Telephone:	+1 (607) 753-6156		E-mail:	peter@systemseast.com
Business Address:	50 Clinton Avenue		City:	Cortland
State/Province:	NY	Country:	USA	Zip: 13045
URL:	https://www.systemseast.com			

#### **Part 1b. Qualified Security Assessor Company Information (if applicable)**

Company Name:	Securisea, Inc.			
Lead QSA Contact Name:	Bill Rudiak		Title:	Director, PCI Programs
Telephone:	+1 (877) 563-4230 x404		E-mail:	brudiak@securisea.com
Business Address:	Suite 1100 – 201 Spear St		City:	San Francisco
State/Province:	CA	Country:	USA	Zip: 94105
URL:	https://www.securisea.com			



## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) assessed: Xpress-pay.com

Type of service(s) assessed:

#### Hosting Provider:

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

#### Managed Services (specify):

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

#### Payment Processing:

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

Account Management

Fraud and Chargeback

Payment Gateway/Switch

Back-Office Services

Issuer Processing

Prepaid Services

Billing Management

Loyalty Programs

Records Management

Clearing and Settlement

Merchant Services

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 you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.



### Part 2a. Scope Verification (continued)

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

Name of service(s) not assessed: Miscellaneous electronic payment services as checked below.

Type of service(s) not assessed:

Hosting Provider:	Managed Services (specify):	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 <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting 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 type="checkbox"/> POS / card present <input 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"/> Back-Office Services <input checked="" type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider <input type="checkbox"/> Others (specify):	<input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input checked="" type="checkbox"/> Merchant Services	<input type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input checked="" type="checkbox"/> Tax/Government Payments

Provide a brief explanation why any checked services were not included in the assessment:

The above checked services do not involve any transmission, processing, or storage of CHD.

### Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Systems East stores, processes, and transmits cardholder data (CHD) entirely within its outsourced cloud environment hosted by Flexential. Systems East's web and application servers running its ecommerce application Xpress-pay.com receive transactions (including CHD) via a TLS-encrypted browser connection and—where necessary for recurring (subscription) billing—encrypts and stores the CHD within a SQL Server database. Systems East transmits CHD for authorization to payment processors or acquirers via the processors' PCI-compliant payment APIs.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

Systems East does not directly or otherwise impact the security of its clients' CDEs other than sharing of CHD which is covered in the scope of the assessment.



### Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
<i>Example: Retail outlets</i>	3	Boston, MA, USA
Corporate Office	1	Cortland, NY

### Part 2d. Payment Applications

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Xpress-pay.com (internally developed payment application)	N/A	Systems East, Inc.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A – Xpress-pay.com is not eligible for PA-DSS certification
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

### Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

The CDE comprises Systems East's web-based ecommerce application (Xpress-pay.com), including web/application/database/ VoIP servers (both production and development), plus supporting technology, i.e. a Vormetric key management virtual appliance. Xpress-pay.com supports acquisition of electronic payments from users (one-time and recurring) and transmits those to one of several upstream payment processors for authorization.



	Systems East outsources management of the infrastructure supporting the payment application (including firewalls, IDS/IPS, logging, and network connections) to Flexential, a cloud-based PCI-validated Level 1 Service Provider.
Does your business use network segmentation to affect the scope of your PCI DSS environment? <i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No



### Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?

Yes  No

**If Yes:**

Name of QIR Company:

QIR Individual Name:

Description of services provided by QIR:

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

Yes  No

**If Yes:**

Name of service provider:	Description of services provided:
Flexential (dba Peak 10, Inc.)	Cloud-based infrastructure hosting
Global Payments Direct; Authorize.Net (Cybersource); EpaymentAmerica; BB&T; Capital One Merchant Services (Vantiv); Forte Payment Systems, Inc.; First Bank of Virgin Islands; EVO Merchant Services; PaymentsGateway.net; MasterCard; Visa, Inc.; TSYS; First Data Merchant Services; TSYS Merchant Services; USA EPAY; Elavon/Converge; US Pay; WorldPay; CoCard; Transaction Express/TransFirst	Payment authorization

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



## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed:		Xpress-pay.com		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Systems East's cloud-based PCI-validated Level 1 service provider (Flexential) has assumed responsibility for requirement 1.2.2 so this requirement is marked N/A.  Requirement 1.2.3 is N/A because there is no wireless within the scope of the CDE.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 2.1.1 is N/A because there is no wireless within scope of the CDE.  Systems East's cloud-based PCI-validated Level 1 service provider (Flexential) has assumed responsibility for requirement 2.2.4 so this requirement is marked N/A.  Requirement 2.6 is N/A because Systems East is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 3.4.1 is N/A because Systems East does not use full disk encryption.  Requirement 3.6.a is N/A because Systems East does not share keys with customers for transmission or storage of CHD.  Requirement 3.6.6 is N/A because Systems East does not use manual clear-text key management operations.





Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Requirement 4.1.1 is N/A because there is no wireless within scope of the CDE.</p> <p>Requirement 4.2 is N/A because Systems East does not use end-user messaging technologies to send CHD.</p>
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Systems East's cloud-based PCI-validated Level 1 service provider (Flexential) has assumed responsibility for requirements 5.1, 5.2, and 5.3 so these requirements are marked N/A.</p>
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Requirement 6.4.4 is N/A because Systems East uses BitBucket which does not migrate test data from development to production.</p> <p>Requirement 6.4.6 is N/A because Systems East has not had a significant change since its last assessment.</p>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Requirement 8.1.3 is N/A because Systems East has not had any terminations of staff with access to the CDE within the past 6 months.</p> <p>Requirement 8.5.1 is N/A because Systems East does not remotely access customer systems.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Systems East's cloud-based PCI-validated Level 1 service provider (Flexential) has assumed responsibility for requirements 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, and 9.8 so these requirements are marked N/A.</p> <p>Requirement 9.9 is N/A because Systems East does not process any card-present transactions.</p>
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Systems East's cloud-based PCI-validated Level 1 service provider (Flexential) has assumed responsibility for requirements 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.4, and 10.5.5 so these requirements are marked N/A.</p>
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Requirement 11.1.1 is N/A because there are no authorized wireless access points within scope of the CDE.</p> <p>Requirement 11.2.3 is N/A because Systems East has not had any significant changes since the previous assessment.</p> <p>Requirement 11.3.3 is N/A because no vulnerabilities were found during the penetration test.</p>



				Systems East's cloud-based PCI-validated Level 1 service provider (Flexential) has assumed responsibility for requirement 11.4 and 11.5 so this requirement is marked N/A.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Systems East is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No POS terminals are within the scope of the CDE.



## Section 2: Report on Compliance

---

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	May 31, 2020
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No



## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated May 31, 2020.

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

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby Systems East, Inc. has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked “Not in Place” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(**Check all that apply**)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, 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 my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.



### Part 3a. Acknowledgement of Status (continued)

<input checked="" type="checkbox"/>	No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Trustwave Holdings, Inc.

### Part 3b. Service Provider Attestation

DocuSigned by: <i>Peter T. Rogati, IV</i> 2E11B814C56C4C0...	
Signature of Service Provider Executive Officer ↑	Date: 6/1/2020
Service Provider Executive Officer Name:	Title: Director of Operations

### Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	Full PCI-DSS Assessment and preparation of Report on Compliance
--	---

DocuSigned by: <i>Josh Daymont</i> CF838494882345C...	
Signature of Duty Authorized Officer of QSA Company ↑	Date: May 31, 2020
Duty Authorized Officer Name: Joshua Daymont	QSA Company: Securisea, Inc.

### Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	
---	--

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

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 a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify 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	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting 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"/>	

