

**Date**

*July 30, 2011*

**Project**

*Attestation of Compliance*

**Client**

*USA800, Inc.*

---

IOActive, Inc.

701 5th Avenue, Suite 6850

Seattle, WA 98104

Toll free: (866) 760-0222

Office: (206) 784-4313

Fax: (206) 784-4367

Copyright ©2010 by IOActive, Incorporated



All Rights Reserved

**Appendix E: Attestation of Compliance – Service Provider**

**Instructions for Submission**

The Qualified Security IOActive (QSA) and Service Provider must complete this document as a declaration of the Service Provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the requesting payment brand.

Part 1. Qualified Security IOActive Company Information					
<b>Company Name:</b>	IOActive, Inc.				
<b>Lead QSA Contact Name:</b>	Frank Osborne	<b>Title:</b>	Senior Consultant		
<b>Telephone:</b>	206-462-4835	<b>Email:</b>	<a href="mailto:fosborne@ioactive.com">fosborne@ioactive.com</a>		
<b>Business Address:</b>	701 5th Avenue, Suite 6850		<b>City:</b>	Seattle	
<b>State/Province:</b>	WA	<b>Country:</b>	USA	<b>ZIP:</b>	98104
<b>URL:</b>	<a href="http://www.ioactive.com">http://www.ioactive.com</a>				
Part 2. Service Provider Organization Information					
<b>Company Name:</b>	USA800, Inc.	<b>DBA(s):</b>	N/A		
<b>Contact Name:</b>	Michael Douglas	<b>Title:</b>	CIO/CTO		
<b>Telephone:</b>	800-821-7539 Ext.207	<b>Email:</b>	<a href="mailto:mdouglas@usa800.com">mdouglas@usa800.com</a>		
<b>Business Address:</b>	6616 Raytown Rd		<b>City:</b>	Raytown	
<b>State/Province:</b>	MO	<b>Country:</b>	USA	<b>ZIP:</b>	64133
<b>URL:</b>	<a href="http://www.usa800.com">http://www.usa800.com</a>				
Part 2a. Services Provided (check all that apply)					
<input type="checkbox"/> Authorization	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> 3-D Secure Access Control Server			
<input type="checkbox"/> Switching Transactions	<input type="checkbox"/> IPSP (E-commerce)	<input type="checkbox"/> Process Magnetic-Stripe			
<input checked="" type="checkbox"/> Payment Gateway	<input type="checkbox"/> Clearing & Settlement	<input checked="" type="checkbox"/> Process MO/TO Transactions			
<input type="checkbox"/> Hosting	<input type="checkbox"/> Issuing Processing	<input type="checkbox"/> Others (please specify):			
List facilities and locations included in PCI DSS review: St. Joseph, Raytown, MO & Halstead, KS					
Part 2b. Relationships					
Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)?					
<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No US800 leverages AT&T managed firewall services-A PCI-DSS approved service provider.					
Part 2c. Transaction Processing					

How and in what capacity does your business store, process and/or transmit cardholder data? Collects, stores and transmits retail customer CHD, PAN, EXP DATE, and for some clients CVV/equivalent, via telephone to client companies for the purpose of purchasing products.	
Payment Application in use:	Custom in-house application.
Payment Application Version:	N/A
<b>Part 3. PCI DSS Validation</b>	
Based on the results noted in the Report on Compliance ("ROC") asserts the following compliance status for the entity identified in Part 2 of this document as of (check one):	
<input checked="" type="checkbox"/>	<b>Compliant:</b> All requirements in the ROC are marked "in place," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor thereby has demonstrated full compliance with the PCI DSS 1.2.
<input type="checkbox"/>	<b>Non-Compliant:</b> Some requirements in the ROC are marked "not in place," resulting in an overall NON-COMPLIANT rating, or a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby has not demonstrated full compliance with the PCI DSS.  <b>Target Date for Compliance:</b>  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, since not all payment brands require this section.</i>
<b>Part 3a. Confirmation of Compliant Status</b>	
<b>QSA and Service Provider confirm:</b>	
<input checked="" type="checkbox"/>	The ROC was completed according to the PCI DSS Requirements and Security Assessment Procedures, Version 1.2, 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"/>	The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
<input checked="" type="checkbox"/>	No evidence of magnetic stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY systems reviewed during this assessment.
<b>Part 3b. QSA and Merchant Acknowledgments</b>	
<b>Signature of Lead QSA:</b>  	<b>Date:</b> 07/30/2011
<b>Lead QSA Name:</b> Frank Osborne	<b>Title:</b> Senior Consultant
<b>Signature of Service Provider Executive Officer:</b>  	<b>Date:</b> 7/30/2011
<b>Service Provider Executive Officer Name:</b>  Mike Douglas	<b>Title:</b> CIO

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "No" to any of the requirements, you are required to provide the date when the item will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. Check with the payment brand(s) before completing Part 4 since not all payment brands require this section.

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (if Compliance Status is "No")
1	Install and maintain a firewall configuration to protect cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
3	Protect stored cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
4	Encrypt transmission of cardholder data across open, public networks.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
5	Use and regularly update anti-virus software.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
6	Develop and maintain secure systems and applications.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
7	Restrict access to cardholder data by business need to know.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
8	Assign a unique ID to each person with computer access.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
9	Restrict physical access to cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
10	Track and monitor all access to network resources and cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
11	Regularly test security systems and processes.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
12	Maintain a policy that addresses information security.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	

