



Attestation of Compliance – Service Providers Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 2.0

October 2010

Instructions for Submission

The Qualified Security Assessor (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. Service Provider and Qualified Security Assessor Information

Service Provider Organization Information

Company Name:	30 Second Software, Inc.	DBA(s):	Digby
Contact Name:	Lance Obermeyer	Title:	CTO
Telephone:	+1-512-826-5001	E-mail:	lanceo@digby.com
Business Address:	3801 S Capital of Tx Hwy Barton Creek Plaza II, Ste 100	City:	Austin
State/Province:	TX	Country:	USA
URL:	http://www.digby.com	Zip:	78704

Qualified Security Assessor Company Information

Company Name:	atsec information security		
Lead QSA Contact Name:	Jeff Jilg	Title:	Senior PCI Manager
Telephone:	+1 512-615-7323	E-mail:	jeff@atsec.com
Business Address:	9130 Jollyville Rd. #260	City:	Austin
State/Province:	TX	Country:	USA
URL:	h	Zip:	78759

Part 2 PCI DSS Assessment Information

Part 2a. Services Provided that WERE INCLUDED in the Scope of the PCI DSS Assessment (check all that apply)

- | | | |
|-------------------------------------------------------|------------------------------------------------------|--------------------------------------------------------|
| <input type="checkbox"/> Payment Processing-POS | <input type="checkbox"/> Tax/Government Payments | <input type="checkbox"/> Fraud and Chargeback Services |
| <input type="checkbox"/> Payment Processing-Internet | <input type="checkbox"/> Payment Processing – ATM | <input type="checkbox"/> Payment Processing – MOTO |
| <input type="checkbox"/> Issuer Processing | <input type="checkbox"/> Payment Gateway/Switch | <input type="checkbox"/> Clearing and Settlement |
| <input type="checkbox"/> Account Management | <input type="checkbox"/> 3-D Secure Hosting Provider | <input type="checkbox"/> Loyalty Programs |
| <input type="checkbox"/> Back Office Services | <input type="checkbox"/> Prepaid Services | <input type="checkbox"/> Merchant Services |
| <input type="checkbox"/> Hosting Provider – Web | <input type="checkbox"/> Managed Services | <input type="checkbox"/> Billing Management |
| <input type="checkbox"/> Network Provider/Transmitter | <input type="checkbox"/> Hosting Provider – Hardware | <input type="checkbox"/> |
| <input type="checkbox"/> Records Management | <input type="checkbox"/> Data Preparation | <input type="checkbox"/> |

Others (please specify): smart phone proxy for online merchants

List facilities and locations included in PCI DSS review:

- offices in Austin, TX and Beijing, China
- data center in Herndon, Virginia (co-located at service provider)

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.)? Yes No

Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data? Smart phone proxy for online merchants: Card Holder Data transmission only
Please provide the following information regarding the Payment Applications your organization uses:

Payment Application in Use	Version Number	Last Validated according to PABP/PA-DSS
Digby Application	N/A, version updated by build number three times weekly	Internally developed application

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated 2011-07-01, *atsec information security* asserts the following compliance status for the entity identified in Part 2 of this document as of 2011-07-01 (check one):

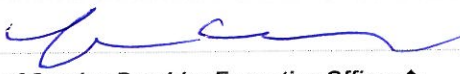
- Compliant:** All requirements in the ROC are marked "in place¹," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor *Alert Logic, Inc.* thereby *Digby* has demonstrated full compliance with the PCI DSS 2.0
- Non-Compliant:** Some requirements in the ROC are marked "not in place," resulting in an overall **NON-COMPLIANT** rating, or a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby (*Service Provider Name*) has not demonstrated full compliance with the PCI DSS.
Target Date for Compliance:
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. *Check with the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA and Service Provider confirm:

- The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures, Version 2.0*, and was completed according to the instructions therein.
- All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
- The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (that is, track) data², CAV2, CVC2, CID, or CVV2 data³, or PIN data⁴ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Service Provider Acknowledgments

	Date: 2011-07-01
Signature of Service Provider Executive Officer ↑	
Service Provider Executive Officer Name: Lance Obermeyer	Title: CTO

¹ "In place" results should include compensating controls reviewed by the QSA. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as "in place."

² 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 magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

³ The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

⁴ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



Jeff Jilg

Signature of Lead QSA ↑

Date: 2011-07-01

Lead QSA Name: Jeff Jilg

Title: PCI Senior Manager (lead
assessor)

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 Company 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	

