Security
Standards Council®

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.0

February 2014

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:	Ecwid, Inc.		DBA (doing business as):	N/A	
Contact Name:	Kirill Kazakov		Title:	Information Security Officer	
ISA Name(s) (if applicable):	N/A		Title:	N/A	
Telephone:	(410) 236-6551		E-mail:	kirikaza@ecwid.com	
Business Address:	144 West D Street, Suite 103		City:	Encinitas	
State/Province:	CA	Country:	USA	Zip:	92024
URL:	www.ecwid.com				

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

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Forrest McMahon		Title:	Director	
Telephone:	(650) 595-9700		E-mail:	forrest.mcmahon@coalfire.com	
Business Address:	361 Centennial Parkway, Suite 150		City:	Louisville	
State/Province:	CO	Country:	USA	Zip:	80027
URL:	www.coalfire.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:	Ecwid E-Commerce Widgets

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.

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:	None	
Type of service(s) not 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):		
Provide a brief explanation why any checked services were not included in the assessment:		

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Ecwid, Inc. (Ecwid) does not store, transmit or process cardholder data within its hosted infrastructure. Ecwid provides a Software-as-a-Service (SaaS) shopping cart widget that can be embedded into customer's website, blog or Facebook page as well as a fully hosted e-commerce store-builder platform. The Ecwid widget, shopping cart, and hosted web sites are cloud-based solutions that are integrated with over 25 payment gateways. Ecwid's web hosting and payment widget systems host the payment web forms only, and all payment transactions with cardholder data, including customer name, address, Primary Account Number (PAN), expiration date, and CVV2, CVC2, CID, or CAV2 are re-directed from merchant customer browsers directly to the merchants' selected third party payment gateway via iFrames or JavaScript API posts. Ecwid receives only the truncated last 4 digits of the PAN for storage; full PAN is not received, stored in databases, or written to disk by Ecwid. Ecwid's merchants process all transactions using their own merchant IDs and all settlement activities and chargebacks are handled directly between the merchants and their selected payment processor and/or acquiring bank.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Ecwid's web hosting and payment widget systems host the payment web forms only. Although, during processing of payment card transactions, cardholder data is transmitted directly from customer browsers to one of the payment gateways via iFrames or JavaScript API posts, the ecommerce widget application and systems can still impact the security of cardholder data. As such, Ecwid, has included all of their web systems and applications within the scope of their Cardholder Data Environment (CDE) and their validation assessment.

Part 2c. Locations

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

Type of facility:	Location(s) of facility (city, country):
Cloud Hosting Production Data Center	Amazon Web Services (AWS) Availability Zones (US-East B, D, & E)

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)
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ 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.*	Ecwid maintains a single production Virtual Private Cloud (VPC) named “Production” hosted using Amazon Web Services (AWS) EC2 and S3 on the AWS availability zones, US-East, Zones B, D, & E. The AWS Management Console (virtual network and firewall management), systems, and applications within the Ecwid production VPC are considered Ecwid’s Cardholder Data Environment (CDE) and are included within the scope of the PCI DSS assessment. Ecwid does not store, process, or transmit cardholder data within its hosting environment. Ecwid hosts the payment web forms and widgets that are displayed to merchant customer’s browsers through their payment widget web application, app.ecwid.com; however, these web forms contain either JavaScript or iFrames provided by the payment processors, and all payment card data is transmitted from the client browsers directly to the payment processor never passing through Ecwid’s systems. The Ecwid merchant control panel web application, my.ecwid.com, allows merchants to configure their shopping cart and payment widget including selecting their payment methods, payment card payment gateway, and entering their Merchant IDs. Cardholder data is not accessible or viewable through this application. All other connections into and out of the Ecwid CDE are for system administration and systems security and monitoring purposes. Remote administrative access to the

	AWS Management Console and into the CDE is enabled with two-factor authentication and all inbound and outbound connections are secured with specific inbound and outbound VPC "firewall" rules limited to that which is necessary.

Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers

Does your company have a relationship with one or more third-party service providers (for example, 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:

Type of service provider:	**Description of services provided:**
Cloud Hosting	Cloud Hosting Infrastructure as a Service

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:	Ecwid E-Commerce Widgets

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	□	☒	□	Requirement(s) 1.1.6 – NA, No insecure ports or protocols are used. Requirement(s) 1.3.7 – NA, Cardholder data is not stored to disk or database by Ecwid.
Requirement 2:	□	☒	□	Requirement(s) 2.1.1 – NA, Wireless networks are not used within or connected to the Ecwid CDE. Requirement(s) 2.2.3 – NA, No unnecessary or insecure services or protocols are used or enabled. Requirement(s) 2.6 – NA, Ecwid is not a shared hosting provider.
Requirement 3:	□	☒	□	Requirement(s) 3.1 – Ecwid does not store cardholder data to disk, database, or on any CDE system components. Requirement(s) 3.2 – NA, Ecwid is not a payment card issuer, does not support or provide issuing services, and does not ever receive or store sensitive authentication data. Requirement(s) 3.4.1, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8 – NA, Cardholder data is not stored to disk or database by Ecwid, therefore, encryption, disk encryption, removable back-up media, and associated key management procedures are not used or necessary within the Ecwid CDE.

Requirement 4:	□	☒	□	Requirement(s) 4.1.1 – NA, Wireless networks are not used within or connected to the Ecwid CDE.
Requirement 5:	□	☒	□	Requirement(s) 5.1, 5.1.1, 5.2, 5.3 – NA, The operating system used by Ecwid for all systems in the CDE, is not commonly affected by viruses in the method in which it is deployed.
Requirement 6:	□	☒	□	6.5.10 – NA, This requirement is considered as a best practice until June 30, 2015.
Requirement 7:	☒	□	□	
Requirement 8:	□	☒	□	Requirement(s) 8.1.5 – NA, Ecwid does not provide any vendors with remote access to their CDE. Requirement(s) 8.5.1 – NA, Ecwid does not provide services that require remote access to customer premises or systems. Requirement(s) 8.7 – NA, No cardholder data is stored to databases, disk, or otherwise within the Ecwid CDE.
Requirement 9:	□	☒	□	Requirement(s) 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2 – NA, Cardholder data is not received, transmitted, processed, or stored by Ecwid; backup media is not used within the Ecwid CDE; and no media containing cardholder data, paper or electronic, is generated or stored by Ecwid. Requirement(s) 9.9, 9.9.1, 9.9.2, 9.9.3 –NA, No card-present transactions are accepted and no card-reading devices are owned or operated by Ecwid.
Requirement 10:	□	☒	□	Requirement(s) 10.2.1 – NA, Ecwid does not directly receive, store, or process cardholder data and does not provide individual user access to cardholder data.
Requirement 11:	□	☒	□	Requirement(s) 11.1.1 – NA, Ecwid does not have any authorized wireless access points within or connected to their CDE.
Requirement 12:	□	☒	□	Requirement(s) 12.9 – NA, This requirement is considered as a best practice until June 30 2015.
Appendix A:	□	☒	□	Requirement(s) Appendix A (all) – NA, Ecwid is not a shared hosting provider.

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:	*6/30/2015*	
Have compensating controls been used to meet any requirement in the ROC?	□ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	□ No
Were any requirements not tested?	□ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	□ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the ROC dated *June 30, 2015*, 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 as of *June 30, 2015*: (***check one)*:**

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Ecwid, Inc.* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company 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.*
☐	**Compliant but with Legal exception:** 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. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.0*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	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)

☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Coalfire Systems, Inc., #3782-01-08*

Part 3b. Service Provider Attestation

Jim O'Hara

Signature of Service Provider Executive Officer ↑	*Date:* 7/8/15
Service Provider Executive Officer Name: Jim O'Hara	*Title:* President

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*Lead QSA - PCI DSS Compliance Advisory and Validation Services*

Forrest McMahon

Signature of QSA ↑	*Date:* 7/9/2015
QSA Name: Forrest McMahon	*QSA Company:* Coalfire Systems, Inc.

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	*N/A*

Signature of ISA ↑	*Date:*
ISA Name:	*Title:*

[1] 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.

[2] 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.

[3] 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	☒	□	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	□	
3	Protect stored cardholder data	☒	□	
4	Encrypt transmission of cardholder data across open, public networks	☒	□	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	□	
6	Develop and maintain secure systems and applications	☒	□	
7	Restrict access to cardholder data by business need to know	☒	□	
8	Identify and authenticate access to system components	☒	□	
9	Restrict physical access to cardholder data	☒	□	
10	Track and monitor all access to network resources and cardholder data	☒	□	
11	Regularly test security systems and processes	☒	□	
12	Maintain a policy that addresses information security for all personnel	☒	□	