Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for
Onsite Assessments – Service Providers

Version 3.2

April 2016

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	
Telephone:	N/A		E-mail:	kirikaza@ecwid.com	
Business Address:	(410) 236-6551		City:	Encitas	
State/Province:	CA	Country:	US	Zip:	92024
URL:	http://www.ecwid.com				

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

Company Name:	Skoda Minotti Risk Advisory Services, LLC				
Lead QSA Contact Name:	Christopher Shaffer		Title:	Sr. Manager	
Telephone:	214.276.1599		E-mail:	cshaffer@skodaminotti.com	
Business Address:	201 East Kennedy Boulevard Suite 1500		City:	Tampa	
State/Province:	FL	Country:	US	Zip:	33602
URL:	http://risk.skodaminotti.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 Platform

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☒ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (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:	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) provides a software-as-a-service product that allows its customers to host payment widgets on their own websites, or as part of their own full service e-commerce webstore offering. Cardholder data that includes the customer name, address, primary account number (PAN), expiration date, and CVV2, CVC2, CID, or CAV2 is transmitted directly from customer browsers to the merchant's (customer) selected payment processors via JavaScript or iFrames that are provided by the selected payment processors directly, or by securely re-transmitting cardholder data directly to the payment processor, having never stored or processed cardholder data.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Ecwid does not store or process cardholder data, but provides payment applications that allow a customer to communicate directly with the payment processor, or by securely re-transmitting chardholder data to the payment processor directly. These payment applications can still impact the security of cardholder data, so Ecwid has chosen to include their entire payment application system within the scope of their Cardholder Data Environment validation 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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Infrastucture as a Service Cloud hosting provider	1	Virginia, US
Infrastucture as a Service Cloud hosting provider	1	Frankfurt, Germany
Infrastucture as a Service Cloud hosting provider	1	Sydney, Australia

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	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ 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's Cardholder Data Environment (CDE) is hosted on the AWS virtual private cloud (VPC) Infrastructure as a Service (IaaS) platform across three availability zones in the AWS US East Region (us-east-1), two availability zones in Europe Central Region (eu-central-1), and three availability zones in the Australia Region (ap-southeast-2). Ecwid does not store or process cardholder data within its hosting environment. Ecwid hosts the payment web forms and widgets that are displayed to merchant customer's browsers; however, these web forms contain either JavaScript or iFrames provided by payment processor, and the payment card data is transmitted from the client browsers directly to the payment processor never passing through Ecwid's systems. Ecwid does have a single payment processing entity where it securely accepts CHD from the client browser, and then securely retransmits CHD to the payment processor, never storing or processing CHD.
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 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:
AWS	Infrastructure services including compute, network, storage and log management.

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:				
	Details of Requirements Assessed			
PCI DSS Requirement	**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:	☐	☒	☐	1.1.6 - Not Applicable – No insecure services, protocols, and ports were used. 1.3.7 - Not Applicable - No CHD is stored to a disk or database.
Requirement 2:	☐	☒	☐	2.1.1 - Not Applicable - Wireless networks are not connected to the CDE. 2.2.3 - Not Applicable - No unnnecessary or insecure services or protocols are in use. 2.6 - Not Applicable - Entity is not a shared hosting provider.
Requirement 3:	☐	☒	☐	3.1 - Not applicable - No CHD is stored to disk or to a database. 3.2 - Not applicable - Entity is not is not a payment card issuer and does not store sensitive data. 3.4.1, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.6, 3.6.1 - 3.6.8 - Not Applicable - Entity does not store CHD to disk or database and therefore removable media and key management procedures are not necessary with the CDE
Requirement 4:	☐	☒	☐	4.1.1 - Not Applicable - Wireless networks are not used within or connected to the CDE.
Requirement 5:	☐	☒	☐	5.1, 5.1.1, 5.2, 5.3 - Not Applicable - Operating systems used within the CDE are not commonly

				affected with viruses based on deployment standards..
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5- Not Applicable - Entity does not provide remote access to CDE to vendors.** **8.5.1 - Not Applicable - Entity does not provide services that require remote access to customer systems.** **8.7 - Not Applicable - No CHD is stored to disk or database wihtin the CDE.**
Requirement 9:	☐	☒	☐	**9.5-9.8.2 - Not Applicable - Entity does not store or process CHD.** **9.9 - 9.9.3 - Not Applicable - Entity does not process card present transactions.**
Requirement 10:	☐	☒	☐	**10.2.1 - Not Applicable - Entity does not store or process CHD and does not provide user access to cardholder data.**
Requirement 11:	☐	☒	☐	**11.1.1 - Not Applicable - Entity does not have authorized wireless connections to or within the CDE.**
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	**Not Applicable - Ecwid is not a shared hosting provider.**
Appendix A2:	☐	☐	☒	**Not Applicable - Ecwid does not use SSL/early TLS.**

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:	*6/29/2017*	
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

This AOC is based on results noted in the ROC dated *6/29/2017*.

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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Ecwid* 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

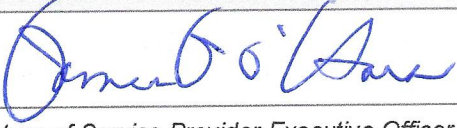## Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2*, 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 & Security Metrics, Inc.*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	Date: **7/7/17**
Service Provider Executive Officer Name: **Jim O'Hara**	*Title:* **President**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*The QSA validated the DSS requirements through testing, inspection, observations, and inquiries and produced a Report on Compliance.*

Christopher Shaffer

Signature of Duly Authorized Officer of QSA Company ↑	Date: *07/05/17*
Duly Authorized Officer Name: Christopher Shaffer	QSA Company: Skoda Minotti Risk Advidory Services, LLC

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:	

---

[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	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	☐	☐	