Appendix C: Attestation of Validation

Instructions for Submission

The Payment Application Qualified Security Assessor (PA-QSA) must complete this document as a declaration of the payment application's validation status with the Payment Application Data Security Standard (PA-DSS). Complete all applicable sections of this Attestation of Validation. Submit the PA-DSS Report on Validation (ROV), this attestation, and the completed PA-DSS Appendix B to PCI SSC. Once accepted by PCI SSC, the payment application will be posted on the PCI SSC website as a PA-DSS validated payment application.

The PA-QSA and Payment Application Software Vendor should complete all sections and submit this document along with copies of all required validation documentation to PCI SSC, per PCI SSC's instructions for report encryption and submission.

Part 1. Payment Application Qualified Security Assessor (PA QSA) Company Information

Company Name:	*Payment Software Company*				
Lead PA-QSA Contact Name:	*Paul Guthrie*	*Title:*	*Partner*		
Telephone:	*+1-408-228-0961 x.101*	*E-mail:*	*paul@paysw.com*		
Business Address:	*1340 DeAnza Blvd #204*	*City:*	*San Jose*		
State/Province:	*CA*	*Country:*	*USA*	*ZIP:*	*95129*
URL:	*http://www.paysw.com*				

Part 2. Payment Application Vendor Information

Company Name:	*Miva Merchant*				
Contact Name:	*Rick Wilson*	*Title:*	*President*		
Telephone:	*+1-858-731-4172*	*E-mail:*	*rwilson@mivamerchant.com*		
Business Address:	*5060 Shoreham Place #33-*	*City:*	*San Diego*		
State/Province:	*CA*	*Country:*	*USA*	*ZIP:*	*92122*
URL:	*http://www.mivamerchant.com*				

Part 2a. Payment Application Information

List Payment Application Name(s) and Version Number(s) included in PA-DSS review:

Payment Application Functionality (check all that apply):

☐ Point of Sale	☒ Shopping Cart	☐ Card-not-present
☐ Middleware	☐ Settlement	☐ Gateway
☐ Automated Fuel Dispenser	☐ Others (please specify):	

Target Market for Application: Internet hosting providers with e-commerce offerings

Part 3. PCI PA-DSS Validation

Part 3a. Confirmation of Validated Status

Based on the results noted in the PA-DSS ROV dated *06/15/2010*, *Payment Software Company* asserts the following validation status for the application(s) and version(s) identified in Part 2a of this document as of *06/15/2010* (check one):

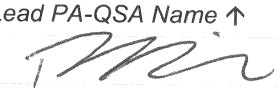
☒	**Fully Validated:** All requirements in the ROV are marked "in place," thereby *Miva Merchant 5.5 PR7 h*as achieved full validation with the Payment Application Data Security Standard.
☒	The ROV was completed according to the PA-DSS, version *1.2.1*, in adherence with the instructions therein.
☒	All information within the above-referenced ROV and in this attestation represents the results of the assessment fairly in all material respects.
☒	No evidence of magnetic stripe (i.e., track) data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization on ANY files or functionalities generated by the application during this PA-DSS assessment.

Part 3b. Annual Re-Validation Confirmation:

	The contents of the above-referenced ROV continue to be applicable to the following software version: *(Payment Application Name and version)*.

Note: Section 3b is for the required Annual Attestation for listed payment applications, and should ONLY be completed if no modifications have been made to the Payment Application covered by the above-referenced ROV.

Part 3c. PA-QSA and Application Vendor Acknowledgments

	06/16/2010
Signature of Lead PA-QSA ↑	*Date* ↑
Paul Guthrie	Partner
Lead PA-QSA Name ↑	*Title* ↑
	06/16/2010
Signature of Application Vendor Executive Officer ↑	*Date* ↑
Rick Wilson	President
Application Vendor Executive Officer Name ↑	*Title* ↑
Miva Merchant	
Application Vendor Company Represented ↑	

[1] Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic stripe data after authorization. The only elements of track data that may be retained are account number, expiration date, and name.

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

[3] PIN Data – Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.