Qualified Integrators and Resellers (QIR)™ Implementation Statement

For each Qualified Installation performed, the QIR Employee must complete this document and confirm whether the validated payment application was installed and configured in accordance with the *PA-DSS Implementation Guide* and in a manner that supports compliance with PCI DSS. A copy of this *QIR Implementation Statement* must be delivered to the customer no later than ten (10) business days after completion of the Qualified Installation, and a copy must be retained by the QIR Company with their work papers.

***Note:** The customer may request the QIR Company to complete work beyond that required to install the payment application and that is outside the scope of the QIR Program. Any such work does not form part of the Qualified Installation.*

The QIR Company must adhere to the requirements defined in the *QIR Qualification Requirements* and *QIR Program Guide* for all Qualified Installations.

Part 1: Implementation Statement Summary

Customer Details					
Company Name:					
Contact Name:			Job Title:		
E-mail:			Telephone:		
Business Address:			City:		
State/Province:		Country:		Postal Code:	
URL:					
QIR Details					
QIR Company Name:					
QIR Primary Contact:			Job Title:		
E-mail:			Telephone:		
Business Address:			City:		
State/Province:		Country:		Postal Code:	
URL:					
PA-DSS Validated Payment Application					
PCI SSC Listing Number:					
Payment Application Vendor:					
Payment Application Name:					
Application Version Number:					

Details of Qualified Installation				
Address of customer location(s) where application was installed	Type of systems application installed on	Number of systems installed	Type of Qualified Installation	Date Installed
			Choose an item.	
			Choose an item.	

Confirmation of Implementation Approach	
This Implementation Statement confirms that:	
The validated payment application was installed in accordance with the ***PA-DSS Implementation Guide.*** *(Yes/No)* *If "No", please provide a brief explanation:*	Choose an item.
The validated payment application was installed and in a manner that supports **compliance with PCI DSS.** ***(****Yes/No)* *If "No", reasons must be documented in Part 3.*	Choose an item.

QIR Acceptance of Implementation Statement	
By accepting this Implementation Statement, *Lead QIR Employee Name* asserts the following for the validated payment application identified above, as of *date:*	
☐	*Lead QIR Employee Name* performed this installation in accordance with the requirements defined in the *QIR Qualification Requirements, QIR Program Guide,* and *QIR Implementation Instructions*.
☐	All information within this Implementation Statement represents the results of the implementation fairly and accurately in all material respects.
☐	*Lead QIR Employee Name* has advised *Customer Company Name* of any potential compliance issues identified during the implementation, as documented in Part 3 of this Implementation Statement.

Lead QIR Employee Signature:			
Lead QIR Employee Name:		*Date:*	

Customer Acceptance of Implementation Statement	
Based on this Implementation Statement, *Customer Company Name* asserts the following for the validated payment application identified above, as of *date* (*each item to be confirmed):*	
☐	*Customer Company Name* accepts the Implementation Result documented above for implementation of the validated payment application implementation.
☐	*Customer Company Name* has read and understands all potential compliance issues identified in Part 3 of this Implementation Statement.
☐	*Customer Company Name* understands they are responsible for maintaining their PCI DSS compliance and that that any changes to the payment application or underlying systems should be made in accordance with PCI DSS Requirements.

Customer Contact Signature:			
Customer Contact Name:		*Date:*	

Part 2: Implementation Statement Details

PA-DSS Implementation Guide and Training Materials Used	
Date and version of the *PA-DSS Implementation Guide* used during the installation of the payment application:	
Details of payment application training materials reviewed prior to the installation (including document name, version, date):	

QIR Access		
1.	Are all QIR personnel using unique accounts and passwords for each customer location?	Choose an item.
2.	Is the customer aware of all accounts set up by or used for QIR personnel access, and have instructions been provided on how to change the passwords and disable or remove those accounts?	Choose an item.

Remote Access		
3.	Is the customer aware that any remote access into their network must be configured as follows:	
	• Remote access to the payment application requires two-factor authentication?	Choose an item.
	• Remote access must be activated only when needed, monitored when in use, and immediately deactivated after use?	Choose an item.
	• Remote access must be implemented securely?	Choose an item.
4.	Will any QIR personnel access the customer site remotely or configure remote access on behalf of the customer?	
☐	**Yes.** QIR Company personnel are using and/or configuring remote access to the customer site:	
	• Is remote access implemented to require two-factor authentication?	Choose an item.
	• Is remote access to the customer network activated only when needed, monitored while in use, and immediately deactivated after use?	Choose an item.
	• Is remote access to the customer network implemented securely?	Choose an item.
☐	**No.** The QIR will not access the customer site remotely and will not configure remote access on behalf of the customer.	

Network Configuration		
5.	Are any external connections required by the payment application?	
☐	**Yes.** The payment application requires external connections:	
	• Is the customer aware of all connections required by the payment application?	Choose an item.
	• Is the customer aware they must use a firewall that allows only required ports on both inbound and outbound connections?	Choose an item.
	• Is the customer is aware that external connections to/from the payment application should only be permitted to specific (known) IP addresses?	Choose an item.
	• Is the customer aware they should enable logging on the firewall?	Choose an item.
☐	**No.** No external connections are required by the payment application.	

Sensitive Authentication Data (SAD)	
6. Is the application configured to ensure that sensitive authentication data (including full track data, card verification codes/values and PIN or PIN block) is <u>not stored</u> after authorization, even if encrypted?	Choose an item.

Troubleshooting and Maintenance		
7. Does the QIR provide services to the customer that could potentially result in the collection of cardholder data and/or sensitive authentication data (for example, for troubleshooting or debugging purposes)?		
☐	**Yes.** The QIR provides services to the customer that could potentially result in the collection of cardholder data and/or sensitive authentication data.	
	• Is sensitive authentication data collected only when needed—and collection limited to only the amount needed—to solve a specific problem?	Choose an item.
	• Is sensitive authentication data stored encrypted in a secure location with limited access?	Choose an item.
	• Is sensitive authentication data securely deleted immediately after use?	Choose an item.
	• Is Primary Account Number (PAN) rendered unreadable when stored?	Choose an item.
☐	**No.** The QIR does not provide any service to the customer that could result in collection of cardholder data and/or sensitive authentication data.	

Protection of Cardholder Data		
8. Does the application store cardholder data?		
☐	**Yes.** The application does store cardholder data.	
	• Is PAN rendered unreadable anywhere it is stored?	Choose an item.
	• Is the customer aware they must securely manage all cryptographic keys?	Choose an item.
	• Is the customer aware they must not store cardholder data on Internet-accessible systems?	Choose an item.
☐	**No.** The application does not store cardholder data.	
9. Is the customer aware that cardholder data must be protected with strong cryptography if sent over public networks or end-user messaging technologies?		Choose an item.
10. Is the customer aware that, if available, encryption of cardholder data transmissions from the customer to back-end processors and/or acquirer is recommended, even for private connections?		Choose an item.
11. Is the customer aware that any non-console administrative access to systems in their cardholder data environment, including payment application must be secured?		Choose an item.

Accounts and Passwords	
12. Have all passwords been changed for all payment application default accounts, and have unnecessary default accounts been removed or disabled (including all user and administrative accounts used by operating systems, software that provides security services, application and system accounts, POS terminals, etc. installed by the QIR Company)?	Choose an item.
13. Is strong authentication configured for all application administrative accounts and for all application accounts with access to cardholder data?	Choose an item.
14. Is the customer aware that all access to systems containing cardholder data (such as PCs, servers, and databases) should use unique user IDs and strong authentication?	Choose an item.
15. Is the customer aware that, for all accounts used by operating systems, security software, application systems, POS terminals, etc.: a. All vendor-supplied defaults should be changed, and b. All unnecessary default accounts should be removed or disabled?	Choose an item.

Logging	
16. Is payment application logging enabled?	Choose an item.
17. Is the customer aware that logs should not be disabled and doing so will result in non-compliance with PCI DSS?	Choose an item.

Wireless		
18. Does the payment application use wireless technology?		
☐	**Yes.** The payment application uses wireless technology.	
	• Is the customer aware that all wireless vendor defaults must be changed?	Choose an item.
	• Is the customer aware they must install and properly configure a firewall between any wireless networks and systems in the cardholder data environment?	Choose an item.
	• Is the customer aware they must implement strong encryption for authentication and transmission of cardholder data over wireless networks?	Choose an item.
☐	**No.** The payment application does not use wireless technology	

Patching	
19. Have the latest vendor-supplied security patches and updates been applied to all software installed by the QIR Employee, including the payment application?	Choose an item.
20. Is the customer aware that vendor-supplied security patches and updates must be applied to the payment application and any underlying software or systems?	Choose an item.

Part 3: QIR Employee Additional Observations

The QIR Employee must use this section to:

- Explain all items identified in Part 2 as *"No – Details provided in Part 3";* and
- Document any observations or details they feel the customer should be aware, including any potential compliance issues the QIR Employee is aware of in the customer environment.

Observation #	Observation Details	Applicable Subject and Question Number from Part 2	Potential PCI DSS compliance issue?		PCI DSS Reference (if applicable)
			Yes	No	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	
			☐	☐	