



Payment Card Industry (PCI) Data Security Standard

NOTE to: BridgePay Gateway & SecureLINK users

**The BridgePay Gateway, used with MobileBytes Services,
is a Payment Gateway, not a Payment Application**

BridgePay Gateway and SecureLINK are products that do not fall under Payment Application Data Security Standard (PA-DSS). PA-DSS is for installed Payment Applications. The Gateway runs on BridgePay systems only, and is covered by the BridgePay PCI-DSS audit. SecureLINK is a part of the BridgePay Gateway. The Gateway is called PathwayLINK.

A copy of BridgePay's Attestation of Compliance is attached to this Cover Statement, listing the BridgePay Gateway as being PCI compliant.



MobileBytes Services does not have access to the Primary Account Number (PAN), as data is encrypted by the reader before reaching MobileBytes. To enable offline transactions when an Internet or Gateway outage occurs, MobileBytes does store encrypted swipe data. MobileBytes does store the cardholder name and expiration date, which is allowed as long as the PAN is not stored (Per PCI DSS Requirement 3, which details the Technical Guidelines for Stored Payment Card Data).





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:	BridgePay Network Solutions, LLC	DBA (doing business as):	T-Gate Payments		
Contact Name:	William Marshall	Title:	Chief Technology Officer		
ISA Name(s) (if applicable):		Title:			
Telephone:	407-960-6464	E-mail:	Bill.Marshall@bridgepaynetwork.com		
Business Address:	600 Northlake Blvd, Suite 210	City:	Altamonte Springs		
State/Province:	Florida	Country:	USA	Zip:	32701
URL:	www.bridgepaynetwork.com				
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	A-lign				
Lead QSA Contact Name:	Lori Crooks	Title:	Managing Consultant		
Telephone:	813-343-0770 Ext 125	E-mail:	Lori.crooks@a-lign.com		
Business Address:	400 N. Ashley Drive Suite 1325	City:	Tampa		
State/Province:	Florida	Country:	USA	Zip:	33602
URL:	www.a-lign.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: Gateway Services

Type of service(s) assessed:

<p>Hosting Provider:</p> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<p>Managed Services (specify):</p> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<p>Payment Processing:</p> <input checked="" type="checkbox"/> POS / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input checked="" type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> 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: Section not applicable

Type of service(s) not assessed:

<p>Hosting Provider:</p> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<p>Managed Services (specify):</p> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<p>Payment Processing:</p> <input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
--	--	--

<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:		

Part 2b. Description of Payment Card Business

<p>Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.</p>	<p>BridgePay Network Solutions (“BridgePay” or the “Company”) provides transaction gateway services to its customers. BridgePay operates two payment gateways, both of which are included in the scope of the assessment. Where testing procedures differ between the two environments A-lign will note the systems as “Legacy” and “BridgePay”. Where a designation is not made, testing procedures covered both environments.</p> <p>The company offers tokenization solutions, which allows customers to process payments without having to handle cardholder data. BridgePay provides a web service using an in house application that serves the card entry user interface (“UI”) through the use of embedded iframes that are easily integrated into the customer’s website. They also accept card data through card swipes or keyed in to a terminal using in house, XAML.</p> <p>Transmit:</p> <p>The payment card data is sent via an TLS encrypted connection to the BridgePay hosted environment. A token is returned to the application and passed to the customers’ application for storage.</p> <p>Store</p> <p>No cardholder data is ever sent to the customers’ database or application. BridgePay stores encrypted CHD for customer payments, and recurring payments within their SQL databases.</p> <p>Process:</p> <p>BridgePay also develops secure payment processing technology to provide integrators with development tools to interface their point-of-sale systems to the BridgePay payment systems. BridgePay connects point-of-sale software integrators with service providers and processors connected to the BridgePay network and merchants with competitive bidding partners that board business on the processors and service providers supported by the BridgePay network. However, BridgePay does not directly process payments.</p>
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p>BridgePay processes credit card payments through a card-not-present and card present channel. Payment information is collected through both of these channels, and the cardholder data is stored encrypted in the databases.</p>

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):
Office facility	Altamonte Springs, FL 32701
Data Center	Orlando, FL 32810

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)
PayLink®	2.1.253	BridgePay	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	Oct 28 2016
PayGuardian	1.1	BridgePay	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	Oct 28 2016
PayGuardian	2.0	BridgePay	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
PathwayLINK™	2.08.1201	BridgePay	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
MyBridgePay	1.2.7	BridgePay	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
BridgeCom	4.3.5	BridgePay	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A

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.

The entire environment is included within the scope of the assessment including:

- Connections into and out of the cardholder data environment (CDE) to/from the customers, as well as the connections to the payment processors.
- The production environment, which includes the databases where the encrypted cardholder data is stored, the web servers and application servers which transmit and assist in the processing of cardholder data.

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:

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:	Gateway Services			
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 2:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 3:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 4:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 9:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not applicable - Inquired of authorized personnel to determine that the organization 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:	May 15, 2015	
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the ROC dated *April 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 *May 15, 2015*: (**check one**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>BridgePay Network Solutions, LLC.</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" data-bbox="289 1493 1409 1652"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

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

<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor

Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑	Date: May 15, 2015
Service Provider Executive Officer Name: William Marshall	Title: Chief Technology Officer

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.

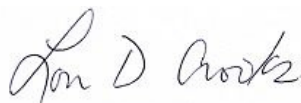
² The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

³ Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

While on-site, the assessor reviewed the physical security of the environment, performed interviews with the technical staff, observed controls in place, and reviewed policies and procedures regarding within scope of the assessment.



Signature of QSA ↑

Date: May 15, 2015

QSA Name: Lori Crooks

QSA Company: A-lign

Part 3d. ISA Acknowledgement (if applicable)

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

Signature of ISA ↑

Date:

ISA Name:

Title:

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

