



Payment Card Industry (PCI) **Data Security Standard**

Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers

For use with PCI DSS Version 3.2.1

July 2018

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-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:	CBV Collection Services Ltd.	DBA (doing business as):	CBV		
Contact Name:	Isak Benjaminsson	Title:	VP - Information Technology		
Telephone:	+1(778) 330-2222	E-mail:	ibenjaminsson@cbvcollections.com		
Business Address:	4664 Lougheed Hwy., Suite 20	City:	Burnaby		
State/Province:	BC	Country:	Canada	Zip:	V5C 5T5
URL:	www.cbvcollections.com				

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

Company Name:	ThreatIQ Inc.				
Lead QSA Contact Name:	Harihar Anand	Title:	Managing Partner ThreatIQ Inc.		
Telephone:	1 866-837-0773 x 202	E-mail:	hari@threatiq.io		
Business Address:	26 Dolby Cres.,	City:	Ajax		
State/Province:	ON	Country:	Canada	Zip:	L1Z 0C9
URL:	www.threatiq.io				

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:	1 st and 3 rd Party Debt Collection Services	
Type of service(s) assessed:		
Hosting Provider: <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):	Managed Services (specify): <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):	Payment Processing: <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 checked="" type="checkbox"/> Others (specify): Entity is contracted by merchants and service providers (3rd party) to collect from debtors via phone. Entity also collects payments on debt owned by entity (1st party)		

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: <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):	Managed Services (specify): <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):	Payment Processing: <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

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	<p>CBV does not store any cardholder data in their environment. Cardholder data is entered in Plently's(PCI Certified Vendor) website directly to complete the transaction.</p> <p>Process:</p> <p>Method 1: Phone-in</p> <ol style="list-style-type: none"> 1. Consumer calls in and CBV's call center agent receives the call. If consumer wishes to make a credit card payment then this call is transferred over to the Payment Processing Team over a non-recorded phone line. 2. Payment Processing Team representative verifies the right party on the account and enters their debt information (EDP, name, amount) in CBV's website. 3. Once validated, they are redirected to Plently's website for secure cardholder transmission and to complete the credit card transaction. 4. Confirmation of payment accepted or rejected is received after the payment is processed on Plently's website.
--	--

	<p>5. Payment Processing Team representative is redirected back to CBV's website.</p> <p>Method 2: Website</p> <ol style="list-style-type: none"> 1. Consumer visits CBV's website and enters their debt information (EDP, name, amount). 2. Once validated, they are redirected to Plently's website for secure cardholder transmission and to complete the credit card transaction. 3. Confirmation of payment accepted or rejected is received after payment is processed on Plently's website. 4. Consumer is redirected back to CBV's website.
<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>CBV Collection Services provides 1st and 3rd party collections to companies across Canada. Some 3rd party clients accept credit cards as payment for debt, while others do not. CBV process the cardholder data via following methods :</p> <ul style="list-style-type: none"> > Phone IN > Website <p>In both methods cardholder transaction happens on Plently's website. Plently is PCI certified and allows for secure cardholder transmission. CBV doesn't store any cardholder data in their environment.</p>

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)
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Datacenter	1	Burnaby, BC, Canada
Office	1	Markham, ON, Canada
Office	1	Laval, QC, Canada

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)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No

Part 2e. Description of Environment

<p>Provide a high-level description of the environment covered by this assessment.</p> <p><i>For example:</i></p> <ul style="list-style-type: none"> • 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. 	<p>CBV's collection services includes the following components within the CDE:</p> <ol style="list-style-type: none"> 1. CBV Payment Processing Team's worksatations 2. CISCO Call Manager System 3. Connection to Pllenty payment processing and authorization 4. Palo Alto Firewall (PA-3220)
---	---

<p>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)</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
---	--

Part 2f. Third-Party Service Providers

<p>Does your company have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated?</p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
--	--

If Yes:

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

Part 2f. Third-Party Service Providers (Continued)

<p>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?</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
--	--

If Yes:

Name of service provider:	Description of services provided:
Pllenty	Payment Processor

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 were assessed for that Requirement, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the SAQ.
- Partial – One or more sub-requirements of that Requirement were marked as “Not Tested” or “Not Applicable” in the SAQ.
- None – All sub-requirements of that Requirement were marked as “Not Tested” and/or “Not Applicable” in the SAQ.

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 SAQ
- 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: CBV 1st and 3rd party collection 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2 - Not Applicable: Router is not present in CBV PCI DSS scoped environment. 1.2.3 - Not Applicable: Wireless Network is not used in CBV environment 1.3.6 - Not Applicable: CBV does not store cardholder data
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - Not Applicable: Wireless Network is not used in CBV environment 2.6 - Not Applicable: Assessed entity is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.2, 3.2.1, 3.2.2, 3.2.3, 3.3, 3.4, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 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, 3.7 - Not Applicable: CBV does not store cardholder data
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - Not Applicable: Cardholder data is not sent over wireless network 4.2 - Not Applicable: Sending PAN over email is not permitted
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.3, 6.3.1, 6.3.2, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10 - Not Applicable:

				CBV does not perform any software development related to cardholder data
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.5 Not Applicable: No remote access by vendors to the assessed environment 8.5.1 - Not Applicable: CBV does not have access to customer environment 8.7 - Not Applicable: CBV does not store cardholder data
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.1.3 - Not Applicable: Wireless Network is not used in CBV environment 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 - Not Applicable: CBV does not store cardholder data 9.9, 9.9.1, 9.9.2, 9.9.3 - Not Applicable: There are no devices that capture payment card data via direct physical interaction in the assessed environment
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.1 - Not Applicable: Wireless Network is not used in CBV environment 11.3.4, 11.3.4.1 - Not Applicable: Segmentation is not implemented in CBV
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3.9, 12.3.10 - Not Applicable: CBV does not store cardholder data
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable - CBV is not a shared hosting provider
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable - No SSL or early TLS is in use in CBV's environment

Section 2: Self-Assessment Questionnaire D – Service Providers

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	03-15-2021	
Have compensating controls been used to meet any requirement in the SAQ?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the SAQ identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements in the SAQ identified as being not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the SAQ 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

This AOC is based on results noted in SAQ D (Section 2), dated 03-15-2021.

Based on the results documented in the SAQ D 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)**:

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>CBV Collection Services Ltd.</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby <i>(Service Provide 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 “No” 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" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">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"/>	PCI DSS Self-Assessment Questionnaire D, Version 3.2.1, was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ 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 <i>Sectigo Limited</i>

Part 3b. Service Provider Attestation

<i>Signature of Service Provider Executive Officer</i> ↑	<i>Date:</i> 04-30-2021
<i>Service Provider Executive Officer Name:</i> Isak Benjaminsson	<i>Title:</i> VP - Information Technology

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA verified compliance of the implemented controls for the in-scope environment for the assessed entity.
--	---

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i> 04-30-2021
<i>Duly Authorized Officer Name:</i> Harihar Anand	<i>QSA Company:</i> ThreatIQ Inc.

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:	No ISA was involved for this assessment
---	---

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	<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"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

