



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

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:	Till Payments Solutions Pty Ltd.	DBA (doing business as):	Till Payments Solutions Pty Ltd in Australia Till Payments, LLC, USA Till Payments Solutions NZ Limited, New Zealand Till Payments Canada Corp. Till Payments Solutions UK Ltd.		
Contact Name:	Shadi Haddad	Title:	Chief Executive Officer		
Telephone:	+61 2 8319 4900	E-mail:	Shadi.Haddad@tillpayments.com		
Business Address:	A L7, 78 Waterloo Road	City:	Macquarie Park		
State/Province:	NSW	Country:	Australia	Zip:	2113
URL:	https://tillpayments.com				

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

Company Name:	Vectra Corporation Ltd.				
Lead QSA Contact Name:	Andrew Deer	Title:	Principal Security Consultant		
Telephone:	+61 8 8208 0800	E-mail:	andrew.deer@vectra-corp.com		
Business Address:	145 South Terrace	City:	Adelaide		
State/Province:	SA	Country:	Australia	Zip:	5000
URL:	www.vectra-corp.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:	E-commerce solutions: Till eCommerce solution, Till Hosted Payments Page, Till Auth CC. Reseller of EFTPOS solutions provided and operated by third party service providers First Data Resources Australia and Fiserve Solutions Europe.
------------------------------	---

Type of service(s) 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):

- | | | |
|--|---|--|
| <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 checked="" type="checkbox"/> Merchant Services | <input 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.

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):

- | | | |
|--|---|--|
| <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.	Till Payments Solutions Pty Ltd (Till Payments) does not store, process or transmit cardholder data. See explanation below for how Till Payments can impact the security of customer 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.	<p>Till Payments’ role is to package, market and resell payment services provided by a number of PCI DSS compliant third parties. This includes:</p> <p>E-commerce – solutions provisioned and managed by ACI Worldwide GmbH PAY.ON.</p> <p>Standalone EFTPOS solutions – provisioned and managed by First Data Resources Australia and Fiserve Solutions Europe.</p> <p>Integrated EFTPOS solutions – provisioned and managed by Fiserve Solutions Europe.</p> <p>Till Payments retains responsibility for managing each of these service providers on behalf of its merchant customers to ensure each one continues to provide PCI DSS compliant in-scope services.</p> <p>Till Payments also hosts ‘web redirection’ infrastructure for a number of merchant customers. The elements of the payment page that collect cardholder data are hosted by IXOPAY and published via an iFrame visible in the customer’s browser.</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>
Head Office	1	Macquarie Park, NSW, Australia
Sales Offices	4	Melville, New York, USA Wellington, New Zealand London, Ontario, Canada London, United Kingdom

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

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.*

Till Payments hosts 'web redirection' infrastructure for a number of merchant customers. The elements of the payment page that collect cardholder data are hosted by PAY IXOPAY and published via an iFrame visible in the customer's browser.

The web redirection infrastructure consists of an Amazon ECS cluster configured as an auto-scaling group and Amazon RDS database hosted in a dedicated Amazon Virtual Private Cloud.

All other in-scope service have been outsourced to in-scope PCI DSS service providers.

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:
ACI Worldwide GmbH (PAY.ON)	Payment processing and related support functions
Amazon Web Services Inc.	Cloud hosting for in-scope web redirection infrastructure
Eftex Pty Ltd	EFTPOS payment switching
First Data Resources Australia Ltd	Provision and management of EFTPOS terminals, payment processing
Fiserv Solutions Europe Ltd	Provision and management of EFTPOS terminals, payment processing
IXOPAY GmbH	Payment gateway, payment processing and support functions

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:	E-commerce solutions: Till eCommerce solution, Till Hosted Payments Page, Till Auth CC. Reseller of EFTPOS solutions provided and operated by third party service providers First Data Resources Australia and Fiserve Solutions Europe.			
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small>
	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 A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Till Payments is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Till Payments does not maintain any POI devices.

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:	<i>28th February 2023</i>	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input 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

This AOC is based on results noted in the ROC dated **16 February 2023**.

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**):

<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>Till Payments Solutions Pty Ltd</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" style="width: 100%; border-collapse: collapse;"> <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"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, 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)

- No evidence of full track data¹, CAV2, CVC2, CVN2, CVV2, or CID data², or PIN data³ 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 (*ASV Name*)

Part 3b. Service Provider Attestation



<i>Signature of Service Provider Executive Officer</i> ↑	Date: 28 February 2023
<i>Service Provider Executive Officer Name:</i> Shadi Haddad	<i>Title:</i> Chief Executive Officer

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

If a QSA was involved or assisted with this assessment, describe the role performed:	<i>The QSA performed examination of documentation, system configurations of the environment. The QSA conducted interviews with technical personnel and stakeholders and prepared the final documentation and completed the Report on Compliance as per PCI SSC guidelines.</i>
--	--

Andrew Deer
Signer ID: 7ACWPF8PH8...

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	Date: 28 February 2023
<i>Duly Authorized Officer Name:</i> Andrew Deer	<i>QSA Company:</i> Vectra Corporation Ltd.

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:	<i>Not Applicable.</i>
---	------------------------

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"/>	









Till Payments 2023 PCI-DSS-v3-2-1-AOC-ServiceProviders-r2 v1_1 (1)

Final Audit Report

2023-02-20

Created:	2023-02-20
By:	Michael Hanna (michael.hanna@tillpayments.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAqZ8-DnpLsbR-Xmu9WruC9r9X4dfT0QTL

"Till Payments 2023 PCI-DSS-v3-2-1-AOC-ServiceProviders-r2 v1_1 (1)" History

-  Document digitally presigned by Foxit Software Inc. (foxit-sign-certs@foxit.com)
2023-02-20 - 5:56:05 AM GMT- IP address: 159.196.127.78
-  Document created by Michael Hanna (michael.hanna@tillpayments.com)
2023-02-20 - 6:07:20 AM GMT- IP address: 159.196.127.78
-  Document emailed to Shadi Haddad (shadi.haddad@tillpayments.com) for signature
2023-02-20 - 6:08:01 AM GMT
-  Email viewed by Shadi Haddad (shadi.haddad@tillpayments.com)
2023-02-20 - 6:25:33 AM GMT- IP address: 104.47.71.254
-  Document e-signed by Shadi Haddad (shadi.haddad@tillpayments.com)
Signature Date: 2023-02-20 - 6:25:57 AM GMT - Time Source: server- IP address: 101.180.90.18
-  Agreement completed.
2023-02-20 - 6:25:57 AM GMT