Payment Card Industry

Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Till Payments Solutions Pty Ltd

Date of Report as noted in the Report on Compliance: 22 September 2025

Date Assessment Ended: 22 September 2025

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)	
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
Company mailing address:	78 Waterloo Road, Macquarie Park, NSW 2113
Company main website:	https://tillpayments.com/
Company contact name:	Michael Hanna
Company contact title:	CIO
Contact phone number:	+61 2 9055 8488
Contact e-mail address:	Michael.Hanna@tillpayments.com

Part 1b. Assessor (ROC Section 1.1)	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable.
Qualified Security Assessor	
Company name:	Vectra Corporation Ltd
Company mailing address:	145 South Terrace Adelaide, South Australia, 5000, Australia
Company website:	www.vectra-corp.com
Lead Assessor name:	Andrew Deer
Assessor phone number:	+61 413 044 246
Assessor e-mail address:	Andrew.Deer@vectra-corp.com

Assessor certificate number:	204-257

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Card present: In-store E-commerce solutions: E-commerce / Online, Till Hosted Payments Page, Till Payment Links / PayByLink (PBL), Till Gateway. 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:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☒ POI / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☒ Clearing and Settlement	☒ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify): Not Applicable.		

Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable.

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Provide a brief explanation why any checked services were not included in the Assessment:	Not Applicable.

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	Till Payments Solutions Pty Ltd (Till Payments) stores and transmits cardholder data for the purpose of its electronic API card payments service. Till Payments does not store, process, or transmit cardholder data for card present payments using Till terminals. This service is outsourced to PCI DSS compliant service providers.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Till payments manage the in-scope AWS environment and are responsible for the configuration of AWS

	services, storage of cardholder data and software development.
Describe system components that could impact the security of account data.	AWS services, including network, authentication, databases, and EC2 hosting of servers may impact the security of cardholder data which transits and is stored in the environment as part of provision of e-commerce and payment terminal services. An EC2 based SFTP server also receives files for settlement purposes. User authentication is provided by Microsoft Azure AD (Microsoft Entra ID).

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	The in-scope environment is entirely contained within the AWS environment, which is located in a dedicated AWS account. An external-facing VPC contains an SFTP service and firewall, which accepts cardholder data before forwarding to an internal VPC where it is temporarily stored in an associate S3 bucket. Truncated cardholder data is retained in a separate S3 bucket. Historical truncated cardholder data is stored within an Azure data lake. An AWS database stores cardholder data used for the Till Payments tokenisation service. Bastion hosts allow access to the environment for systems management purposes. AWS logging and monitoring services are utilised for security purposes, with a third-party SIEM service managing security monitoring and alerting. Private links are maintained to partner payment services. A Cloudflare WAF service is utilised for web application firewall purposes.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Data centres	2	Sydney, Australia
Head Office	1	Macquarie Park, NSW, Australia
Sales Offices	4	Melville, New York, USA Wellington, New Zealand Montreal, Quebec, Canada London, Unted Kingdom

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☒ Yes ☐ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
PAX	A920	PTS Devices	4-40215	2026-04-30
Verifone	T650p	PTS Devices	4-30400	2026-04-30

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services	Data centre and compute services
FIS	Payment processing and software development
Microsoft Azure	Authentication services
Rapid7	SIEM services
Cloudflare	Web application firewall
Fiserv	Merchant payment processing
Linkly	Terminal software provider
Eftex	Merchant payment processing
PAX	Remote key injection facility
IXOPAY TNS ACI PAY.ON Stickman Services	Merchant payment processing Data communications services Payment processing SOC services

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

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: Card present, card-not-present payments, tokenisation services

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	☒	☒	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☒	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6 No insecure services, ports, or protocols are in use. 1.3.3 No wireless networks are present. 2.2.5 No insecure services, protocols, or daemons are in use. 2.3.1, 2.3.2 No wireless networks are present. 3.3.3 Till Payments is not an issuer or company that supports issuing services. 3.5.1.2, 3.5.1.3 No disk or partition-level encryption is in use. 3.7.6 No manual cleartext cryptographic key-management operations are in use. 3.7.9 Till payments do not distribute keys to customers. 4.2.1.2 No wireless networks are present. 4.2.2 No end-user messaging technologies are used to transmit cardholder data. 5.2.3.1 All system components have anti-malware installed on them. 5.3.2.1 Continuous behavioural analysis is in place. 6.4.1 This requirement is superseded by requirement 6.4.2 as of 31 March 2025. 7.2.6 There is no user access to query cardholder data. 8.2.3 Till Payments do not have remote access to customer premises. 8.3.10.x No customer user access to cardholder data is in use. 8.3.11 No physical or logical tokens are in use for authentication. 9.2.x, 9.3.x These requirements are the responsibility of the PCI DSS compliant service provider. 9.4.x No media contains cardholder data. 9.4.1.1, 9.4.1.2 No cardholder data is stored on removable or offline media or exported outside the AWS environment. The AWS PCI DSS compliance meets this requirement for the underlying AWS infrastructure and services. 9.5.1.2.x These requirements are the responsibility of the merchants. 10.4.2.x All logs are reviewed daily via automated means. 10.7.2 This requirement is superseded by requirement 10.7.2 as of 31 March 2025. 11.2.x No wireless networks are in scope. The environment exists within the AWS cloud. AWS PCI DSS compliance supports this requirement. 11.4.5, 11.4.6 No segmentation is in use. The environment is hosted in a dedicated AWS environment. AWS PCI DSS compliance supports segmentation for the underlying AWS infrastructure. 11.4.7 Till Payments is not a multi-tenant service provider. 12.3.2 No requirements are met by customised approach methods in the assessment.

For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable.

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2025-06-25
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-09-22
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2025-09-22)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)*:

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby Till Payments Solutions Pty Ltd has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Michael Hanna

Signature of Service Provider Executive Officer ↑	Date: 2025-09-22
Service Provider Executive Officer Name: Michael Hanna	Title: Chief Information Officer

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	Date: 2025-09-22
Lead QSA Name: Andrew Deer	

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2025-09-22
Duly Authorized Officer Name: Kelvin Heath	QSA Company: Vectra Corporation

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

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 network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/