

Payment Card Industry Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire A

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: January 2025



Section 1: Assessment Information

Instructions for Submission

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

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information		
Part 1a. Assessed Merchant		
Company name:	Fancy Rentals LLC	
DBA (doing business as):	Fancy Rentals	
Company mailing address:	298 N Plainfield Rd, Lebanon, NH 03766	
Company main website:	https://www.fancyrentals.com/	
Company contact name:	Fancy Rental	
Company contact title:	Owner	
Contact phone number:	(603) 298-6884	
Contact e-mail address:	fancy@fancyrentals.com	

Part 1b. Assessor

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:	Not Applicable
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	



Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):		
Indicate all payment channels use	d by the business that are included in this assessment.	
Mail order/telephone order (MOTO	0)	
☐ ✓ E-Commerce		
☐ Card-present		
Are any payment channels not included in this assessment?	□ Yes □ ✓ No	
If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.		
Note: If the organization has a p	ayment channel that is not covered by this SAQ, consult with the entity(ies) to	

Note: If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data
OwnerRez	OwnerRez is PCI compliant and certified, and securely encrypts and stores credit card information.

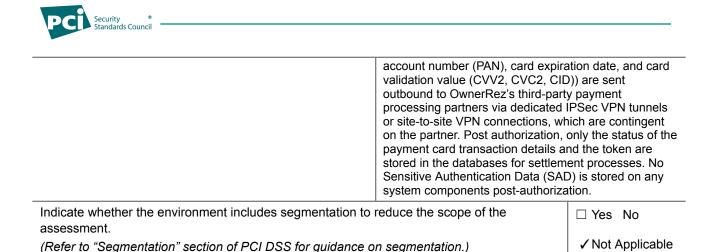
Part 2c. Description of Payment Card Environment

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.

OwnerRez is a property management software designed for vacation rental businesses of all sizes. It enables short-term rental owners and property managers to securely accept card-not-present payments through the app.ownerrez.com endpoint. OwnerRez's service (app.ownerrez.com) enables card-not-present payment transactions for vacation rental owners and property managers by connecting them to third-party payment processors (e.g., Stripe, Lynnbrook Group, etc.) to provide secure tokenized API service to process credit card transactions. The API code allows the cardholder details such as name, address, primary account number (PAN), card expiration date, and card validation value (CVV2, CVC2, CID) that are collected to be transmitted securely via HTTPS using TLS to OwnerRez. OwnerRez vaults cardholder data within a token vault database using strong encryption. For payment processing, cardholder data details (such as primary



Part 2. Executive Summary (continued)

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers, and mail rooms) in scope for the PCI DSS 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
Not Applicable		
Part 2e. PCI SSC Validated Prod	ducts and Solutions	
Does the merchant use any item ide ☐ Yes ☐ No ✓ Not Applicable	entified on any PCI SSC Lists of Valida	ated Products and Solutions ¹ *?
Provide the following information re Products and Solutions.	garding each item the merchant uses	from PCI SSC's Lists of Validated

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.



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 (YYYY-MM-DD)
Not Applicable				YYYY-MM-DD
				YYYY-MM-DD

Pa	rt 2. Executive Summary (continued)			
Pa	rt 2f. Third-Party Service Providers			
С	oes the merchant have relationships with o	ne or more third-party service providers that:		
•		on the merchant's behalf (for example, payment service providers (PSPs), and off-site storage)	□ ✓ Yes	□ No
•		curity control services, anti-malware services, (SIEM), contact and call centers, web-hosting	□ ✓ Yes	□ No
•	Could impact the security of the merchant support via remote access, and/or bespok		□ Yes	✓ □ No
If Y	es:			
Na	me of service provider:	Description of service(s) provided:		
Oı	wnerRez	Provides secure card-not-present payments throug app.ownerrez.com endpoint.	h the	



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



Part 2. Executive Summary (continued)

Part 2g. Summary of Assessment

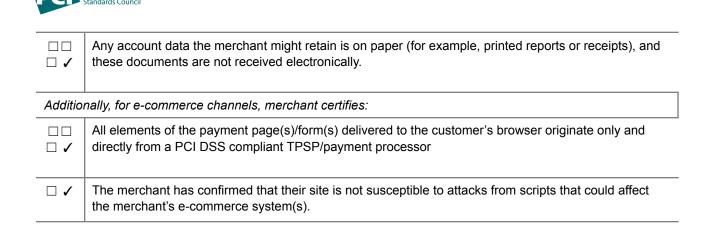
(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS	More that	Requirement on one response may be Indicate all respo	selected for a given req	uirement.
Requirement *	In Place	In Place with CCW	Not Applicable	Not in Place
Requirement 2:				
Requirement 3:	□ ✓			
Requirement 6:				
Requirement 8:	□ ✓			
Requirement 9:				
Requirement 11:	□ ✓			
Requirement 12:	□✓			

^{*} PCI DSS Requirements indicated above refer to the requirements in Section 2 of the SAQ associated with this AOC.

Part 2l	h. Eligibility to Complete SAQ A
Mercha	ant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment channel:
□ □ ✓	The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
	All processing of account data is entirely outsourced to a PCI DSS compliant third-party service provider (TPSP)/payment processor;
	The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions;
	The merchant has confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant;





Section 2: Self-Assessment Questionnaire A

Self-assessment completion date:	2025-03-01	
Were any requirements in the SAQ unable to be met due to a legal constraint?	□ Yes No	✓ □



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ A (Section 2), dated (Self-assessment completion date 2025-03-01).

Based on the results documented in the SAQ A noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

0-	lect		
JE	CLL	UII	┖.

Compliant: All sections of the PCI DSS SAQ are complete and all requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall COMPLIANT rating; thereby (<i>Fancy Rentals</i>) has demonstrated compliance with all PCI DSS requirements included in this SAQ.		
Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall NON-COMPLIANT rating; thereby (Merchant Company Name) has not demonstrated compliance with the PCI DSS requirements included in this SAQ.		
	n with a Non-Compliant status may be required to complete the Action Confirm with the entity to which this AOC will be submitted before	
Compliant but with Legal exception: One or more requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby (Merchant Company Name) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted 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 3a. Merchant Acknowledgement							
Signatory(s) confirms: (Select all that apply)							
	PCI DSS Self-Assessment Questionnaire A, Version 4.0.1, was completed according to the instructions therein.						
	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.						
	PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.						
Part 3b. Merchant Attestation							
Sign	ature of Merchant Executive Officer		Date: 2025-03-01				
Merchant Executive Officer Name: Fancy Rental			Title: Owner				
Part 3c. Qualified Security Assessor (QSA) Acknowledgement							
	QSA was involved or assisted with	☐ QSA performed testing procedures.					
this assessment, indicate the role performed:		☐ QSA provided other assistance.					
		If selected, describe all role(s) performed:					
Signature of Lead QSA □			Date: YYYY-MM-DD				
Lead QSA Name:							
Signature of Duly Authorized Officer of QSA Company			Date: YYYY-MM-DD				
Duly Authorized Officer Name:			QSA Company:				
Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement							
	ISA(s) was involved or assisted with	☐ ISA(s) performed testing procedures.					
this a	assessment, indicate the role ormed:	☐ ISA(s) provided other assistance.					
репс		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 a Non-Compliant status 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 merchant expects to be compliant with the requirement and 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
		YES	NO	Requirement)
2	Apply secure configurations to all system components			
3	Protect stored account data			
6	Develop and maintain secure systems and software			
8	Identify users and authenticate access to system components			
9	Restrict physical access to cardholder data			
11	Test security systems and networks regularly			
12	Support information security with organizational policies and programs			

^{*} PCI DSS Requirements indicated above refer to the requirements in Section 2 of the SAQ associated with this AOC.

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 its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.