



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance - Merchants

Version 4.0.1

Publication Date: August 2024



PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance - Merchants

Entity Name: Prog Leasing, LLC

Date of Report as noted in the Report on Compliance: 2025-03-28

Date Assessment Ended: 2025-03-24



Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the merchant's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* ("Assessment"). 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 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:	Prog Leasing, LLC
DBA (doing business as):	
Company mailing address:	256 West Data Dr., Draper, UT 84020
Company main website:	www.progleasing.com
Company contact name:	Diego Souza
Company contact title:	Chief Information Security Officer
Contact phone number:	(801) 316-6771
Contact e-mail address:	diego.souza@progleasing.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:	SecurityMetrics, Inc.
Company mailing address:	1275 W 1600 N, Orem, UT 84057
Company website:	www.securitymetrics.com
Lead Assessor name:	Michael Simpson
Assessor phone number:	(801) 705-5647
Assessor e-mail address:	aoc@securitymetrics.com
Assessor certificate number:	202-108



Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):
(ROC Sections 2.1 and 3.1)

Indicate all payment channels used by the business that are included in this Assessment.

- ☒ Mail order / telephone order (MOTO)
- ☒ E-Commerce
- ☐ Card-present

Are any payment channels not included in this Assessment?

If yes, indicate which channel(s) is not included in the Assessment and provide a brief explanation about why the channel was excluded.

☐ Yes ☒ No

Not Applicable

Note: If the merchant has a payment channel that is not covered by this Assessment, 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
(ROC Sections 2.1 and 3.1)

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
E-Commerce	As part of Prog Leasing’s lease-purchase/rent-to-own business functions, cardholder data is captured during the application process and as customers make ongoing payments to their account. Cardholder data is received via online (web and mobile) transactions, through web API connections with retail partners. Data captured is transmitted to Ixopay for tokenization and to Fiserv for processing.
Telephone Order	Telephone-order transactions use an automated IVR with tone masking technology provided by the hosted Genesys Cloud solution.

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 Prog Leasing CDE consists of code running in the AWS Lambda API Gateway, AWS S3 and RDS storage, and a hosted IVR and contact center solution provided by Genesys Telecommunications Laboratories.

All connections coming into the AWS-hosted CDE pass through the Imperva-hosted web application firewall.

The CDE connects to Ixopay for tokenization and to Fiserv for payment processing.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment.

Refer to “Segmentation” section of PCI DSS for guidance on segmentation.

☐ Yes ☒ No



Part 2. Executive Summary (continued)

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

List all types of physical locations/ facilities (for example, retail locations, 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: Retail locations	3	Boston, MA, USA
AWS Cloud Hosting	1	AWS US-WEST & US-EAST

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
Not Applicable				

* 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)

Does the entity have relationships with one or more third-party service providers that:	
<ul style="list-style-type: none">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)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none">Manage system components included in the scope of the Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none">Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Service(s) Provided:
Fiserv	Payment Processing
Ixopay, Inc. (TokenEx)	Tokenization Services
Amazon Web Service (AWS)	Cloud Hosting and Security Solutions
Imperva	Web Application Firewall
Okta	Authentication Services
Genesys Telecommunications Laboratories, Inc.	Cloud-Hosted IVR and Contact Center Solution

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.

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:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i>	2024-10-31
Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i>	2025-03-24
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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 2025-03-28).

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):

<input checked="" type="checkbox"/>	<p>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 <i>Prog Leasing, LLC</i> has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>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 (<i>Merchant Company Name</i>) has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance: YYYY-MM-DD</p> <p>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.</p>								
<input type="checkbox"/>	<p>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 (<i>Merchant Company Name</i>) 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.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table><thead><tr><th>Affected Requirement</th><th>Details of how legal constraint prevents requirement from being met</th></tr></thead><tbody><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></tbody></table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								



Part 3. PCI DSS Validation (continued)

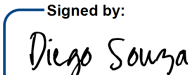
Part 3a. Merchant Acknowledgement

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. Merchant Attestation

Signed by:

3F31D9B477B940B...
Signature of Merchant Executive Officer ↑

Date: 3/28/2025 | 09:43 MDT


Merchant Executive Officer Name: Diego Souza

Title: Chief Information Security Officer

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

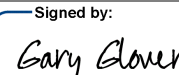
If a QSA was involved or assisted with this Assessment, indicate the role performed:

☒ QSA performed testing procedures.
☐ QSA provided other assistance.
If selected, describe all role(s) performed:

DocuSigned by:

4CB9A1BFFFE542D...
Signature of Lead QSA ↑

Date: 3/28/2025 | 08:45 PDT

Lead QSA Name: Michael Simpson

Signed by:

490DC91BF4FD4DF...
Signature of Duly Authorized Officer of QSA Company ↑

Date: 3/28/2025 | 09:42 MDT

Duly Authorized Officer Name: Gary Glover

QSA Company: SecurityMetrics, Inc.

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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input 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 type="checkbox"/>	<input type="checkbox"/>	

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/