



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Merchants

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 merchant's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact your acquirer (merchant bank) or the payment brands for reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:	Grammarly, Inc	DBA (doing business as):	N/A		
Contact Name:	Alan Luk	Title:	GRC Manager		
Telephone:	+1 206-227-6569	E-mail:	Alan.luk@grammarly.com		
Business Address:	548 Market Street, #35410	City:	San Francisco		
State/Province:	California	Country:	USA	Zip:	94104
URL:	https://www.grammarly.com/				

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

Company Name:	Protiviti				
Lead QSA Contact Name:	Chip Wolford	Title:	Managing Director		
Telephone:	+1 513-362-1716	E-mail:	Chip.wolford@protiviti.com		
Business Address:	201 E Fifth St., Suite 700	City:	Cincinnati		
State/Province:	Ohio	Country:	United States of America	Zip:	45202
URL:	https://www.protiviti.com/				

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

- Retailer
 Telecommunication
 Grocery and Supermarkets
 Petroleum
 E-Commerce
 Mail order/telephone order (MOTO)
 Others (please specify):

What types of payment channels does your business serve?

- Mail order/telephone order (MOTO)
 E-Commerce
 Card-present (face-to-face)

Which payment channels are covered by this assessment?

- Mail order/telephone order (MOTO)
 E-Commerce
 Card-present (face-to-face)

Note: If your organization has a payment channel or process that is not covered by this assessment, consult your acquirer or payment brand about validation for the other channels.

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

Grammarly develops generative AI solutions that help people communicate effectively in written English. Grammarly's AI-enabled English communication technology is available to multiple user groups – Individual Users, Enterprises and Educational users. Through machine learning and deep learning algorithms, Grammarly's product offers grammar checking, spell checking, and plagiarism detection services and suggestions about writing clarity, concision, vocabulary, delivery style, and tone.

Grammarly sells its software through its online website – Grammarly.com and accepts payments using payment cards and invoices. The scope of this assessment covers all transactions involving payment cards which originate through its website.

No cardholder data is stored, processed, or transmitted by Grammarly services or staff members. All processing and transmission of cardholder data are managed by PCI DSS validated service providers - Braintree and Stripe.

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>
Amazon Web Services (AWS) Data Center Region	2	Amazon Web Services, US West High Availability Zone

Part 2d. Payment Application

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)
Not Applicable	N/A	N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No	N/A

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*

All credit card payments are processed by PCI DSS validated service providers - Braintree and Stripe.

Grammarly's infrastructure is hosted on AWS.

To subscribe to Grammarly's software service, customers choose a subscription

<i>devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i>	<p>plan and enter payment card details in a payment form rendered in an iFrame originating from its payment processors – Stripe and Braintree.</p> <p>No CHD is stored, processed, or transmitted by Grammarly services or staff members.</p>
--	---

<p>Does your business use network segmentation to affect the scope of your PCI DSS environment? <i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i></p>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
--	---

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
--	---

If Yes:

Name of QIR Company:	N/A
QIR Individual Name:	N/A
Description of services provided by QIR:	N/A

Does your company share cardholder data with any 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.)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
---	---

If Yes:

Name of service provider:	Description of services provided:
Amazon Web Services	Managed Hosting Provider
Stripe	Payment Service Provider
Braintree	Payment Service Provider

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

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:	17 November 2023
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 17 November 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 Grammarly, Inc 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>Merchant 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 your acquirer or 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: 30%;">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 v3.2.1 , 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 checked="" 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, CVN2, CVV2, or CID data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment.
<input type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>not applicable</i>


Part 3b. Merchant Attestation

DocuSigned by:

 3DF4509F148E4C0...

<i>Signature of Merchant Executive Officer</i> ↑	<i>Date:</i> 17 November 2023
<i>Merchant Executive Officer Name:</i> Alan Luk	<i>Title:</i> GRC Manager

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSAs from Protiviti were involved in the assessment and completion of the ROC.
--	--

DocuSigned by:

 61BBEDA61C5F415...

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i> 17 November 2023
<i>Duly Authorized Officer Name:</i> Chip Wolford	<i>QSA Company:</i> Protiviti

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:	Not Applicable
---	----------------

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 your acquirer or the 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 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"/>	

