Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire A

For use with PCI DSS Version 3.2.1

July 2018

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-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 to determine 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:	Head of GRC	
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://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, Cincinnati		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?	Which payment channels are covered by this SAQ?
☐ Mail order/telephone order (MOTO)	☐ Mail order/telephone order (MOTO)
☒ E-Commerce	☒ E-Commerce
☐ Card-present (face-to-face)	☐ Card-present (face-to-face)

Note: *If your organization has a payment channel or process that is not covered by this SAQ, 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 is a multinational technology company that develops paid subscription software, an English language digital writing tool using artificial intelligence and natural language processing. Through machine learning and deep learning algorithms, Grammarly's product offers grammar checking, spell checking, and plagiarism detection services along with suggestions about writing clarity, concision, vocabulary, delivery style, and tone. No CHD 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)
Example: Retail outlets	*3*	*Boston, MA, USA*
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			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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.*	All credit card payments are processed by PCI DSS-validated service providers, Braintree and Stripe. To subscribe to Grammarly's software service, customers choose a subscription plan and input payment card details in the iframe which is hosted by Braintree. Grammarly uses Stripe's hosted payment page to securely collect invoice payments from their customers. No CHD is stored, processed or transmitted by Grammarly services or staff members. All payment pages delivered to the customer's browser originate directly from the payment service providers - Braintree and Stripe
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 use a Qualified Integrator & Reseller (QIR)?	☐ Yes ☒ No

If Yes:

Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	

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.)?	☒ Yes ☐ No

If Yes:

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

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

Part 2g. Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because, for this payment channel:

☒	Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions);
☒	All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
☒	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
☒	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
☒	Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.
☒	*Additionally, for e-commerce channels:* All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

Section 2: Self-Assessment Questionnaire A

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	18th November 2022	
Have compensating controls been used to meet any requirement in the SAQ?	☐ Yes	☒ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☒ Yes	☐ No
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 *18th November 2022.*

Based on the results documented in the SAQ A 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):***

☒	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Grammarly, Inc* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Merchant Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: 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. *Check with your acquirer or the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	PCI DSS Self-Assessment Questionnaire A, Version *v3.2.1*, was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	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 data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] 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 *not applicable*

Part 3b. Merchant Attestation

DocuSigned by:
Alan Luk
3DF4509F148E4C0...

Signature of Merchant Executive Officer ↗	*Date:* **18th November 2022**
Merchant Executive Officer Name: **Alan Luk**	*Title:* **Head of GRC**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA spent time on walkthrough cardholder dataflow and network infrastructure, and scope validation in September 2022. Afterwards, QSA performed remote assessment activities, including additional sampling testing, documentation review and follow-up interviews until completion date of the SAQ A.

DocuSigned by:
Chip Wolford
61BBEDA61C5F415...

Signature of Duly Authorized Officer of QSA Company ↗	*Date:* **18th November 2022**
Duly Authorized Officer Name: **Chip Wolford**	*QSA Company:* **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	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	

** PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.*