Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	Rebilly, Inc.		DBA (doing business as):	Rebilly, SRL	
Contact Name:	Samuel Lafrenaye Lamontagne		Title:	DevOPS Security Manager	
Telephone:	+1 (512) 710 1640		E-mail:	samuel@rebilly.com	
Business Address:	ISL Complex, Warrens Industrial Park		City:	St. Michael	
State/Province:	N/A	Country:	Barbados	Zip:	N/A
URL:	www.rebilly.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Dara Security				
Lead QSA Contact Name:	William C Kincaid		Title:	Sr Info Sec Analyst	
Telephone:	719 445 9026		E-mail:	wkincaid@darasecurity.com	
Business Address:	10580 N. McCarran Blvd Suite 115-337		City:	Reno	
State/Province:	NV	Country:	USA	Zip:	89503
URL:	www.darasecurity.com				

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Rebilly Saas Cloud Based Billing Service for Subscription Businesses	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☒ Other processing (specify): Recurring
☐ 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):		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) not assessed:	N/A	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (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:		

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Rebilly is a payment gateway that accepts transactions via proprietary API (https://api.rebillly.com) through AWS and on to one of several destinations/acquirers. Once authorization is received Rebilly returns a token to the merchant via their API.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Rebilly stores CHD for recurring billing and for token conversion related to chargeback management

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

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*
Corp Offices (SW Dev, Sys Admins)	1	Montreal, QC, Canada
Corp Offices (SW Dev, Sys Admins)	1	Austin, TX, USA

Part 2d. Payment Applications

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)
In-House		Self-Developed	☐ Yes ☒ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ 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.*	Assessment addressed all system components within the CDE to include database servers, application servers, and web servers. Assessment covered connection to payment processors and development of the software used by entity in delivery of their services. Assessment also covered implemented policies and procedures governing security and PCI DSS compliance
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

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	
QIR Individual Name:	
Description of services provided by QIR:	
Does your company have a relationship with one or more 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.) for the purpose of the services being validated?	☒ Yes ☐ No
If Yes:	

Name of service provider:	**Description of services provided:**
A1Gateway	Payment Gateway
Adyen	
Airpay	
AmazonPay	
AmexVPC	
ApcoPay	
AsiaPaymentGateway	
AstroPayCard	
AuthorizeNet	
Bambora	
BitPay	
BlueSnap	
BraintreePayments	
Cardknox	
Cashflows	
CASHlib	
CashToCode	
CauriPayment	
Cayan	
CCAvenue	
Chase	
CheckoutCom	
Circle	
Citadel	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

Clearhaus	
CODVoucher	
CoinGate	
CoinPayments	
Conekta	
Coppr	
Credorax	
Cryptonator	
CyberSource	
DataCash	
Dengi	
Directa24	
dLocal	
Dragonphoenix	
EBANX	
ecoPayz	
EcorePay	
Elavon	
eMerchantPay	
EMS	
EPG	
EPro	
Euteller	
eZeeWallet	
ezyEFT	
Finrax	
FinTecSystems	
Flexepin	
Forte	
FundSend	
GET	
Gigadat	
GlobalOnePay	
Gooney	
Gpaysafe	
Greenbox	
HiPay	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

iCanPay	
ICEPAY	
iCheque	
iDebit	
Ilixium	
Ingenico	
INOVAPAY	
Inovio	
InstaDebit	
Intuit	
IpayOptions	
Jeton	
JetPay	
Khelocard	
Konnektive	
loonie	
LPG	
MiFinity	
Moneris	
MtaPay	
MuchBetter	
MyFatoorah	
Neosurf	
Netbanking	
Neteller	
NGenius	
NinjaWallet	
NMI	
NuaPay	
OchaPay	
Onlineueberweisen	
OnRamp	
Pagsmile	
Panamerican	
ParamountEft	
ParamountInterac	
Pay4Fun	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

PayCash	
PayClub	
Payeezy	
Payflow	
PaymentAsia	
PaymenTechnologies	
PaymentsOS	
Paymero	
Paynote	
PayPal	
Payr	
Paysafe	
Paysafecash	
PayTabs	
PayULatam	
Payvision	
Piastrix	
Plugnpay	
PostFinance	
Prosa	
Rapyd	
Realex	
Realtime	
Redsys	
Rotessa	
RPN	
Safecharge	
Sagepay	
SaltarPay	
SeamlessChex	
SecureTrading	
SecurionPay	
Skrill	
SmartInvoice	
SMSVoucher	
Sofort	
SparkPay	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

Stripe	
TeIr	
ToditoCash	
Truevo	
Trustly	
TrustPay	
TrustsPay	
TWINT	
UPayCard	
USAePay	
VantivLitle	
VCreditos	
vegaaH	
Wallet88	
Walpay	
Wirecard	
WorldlineAtosFrankfurt	
Worldpay	
XPay	
Zimpler	
Zotapay	
Note: *Requirement 12.8 applies to all entities in this list.*	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

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:	Rebilly

PCI DSS Requirement	Details of Requirements Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	☐	☐	
Requirement 2:	☐	☒	☐	2.6 Entity is not a Hosting Provider
Requirement 3:	☐	☒	☐	3.2 Entity is not an Issuer 3.4.1 Disk Encryption not utilized in environment
Requirement 4:	☐	☒	☐	4.1.1 Entity does not have wireless deployed within CDE
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.5.1 Entity does not maintain access to consumer customer environments
Requirement 9:	☐	☒	☐	9.9-9.9.3 Entity does not maintain or deploy POI devices
Requirement 10:	☒	☐	☐	
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☒	☐	☐	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

Appendix A2:	☒	☐	☐	

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

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:	*08/6/2021*	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *08/5/2020.*

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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Rebilly SRL has demonstrated full compliance with the PCI DSS.
☐	**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 *(Service Provider 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 the payment brand(s) before completing Part 4.*
☐	**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. *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)

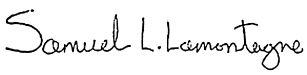
☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all 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.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

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 *Security Metrics*

Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑	*Date: 08/6/2021*
Service Provider Executive Officer Name: Samuel Lafrenaye Lamontagne	*Title:* DevOPS Security Manager

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Performed PCI Assessment using PCI DSS Version 3.2.1

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 08/6/2021*
Duly Authorized Officer Name: William C Kincaid	*QSA Company: Dara Security*

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:	

[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.

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

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 the applicable 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	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	N/A
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	N/A

© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved.

Doc ID: c0e0ba1850b5a899cf53c98a267c8075a14dee24

HELLOSIGN

Audit Trail

TITLE	Rebilly Aug 2021 PCI DSS AOC
FILE NAME	PCI-DSS-v3_2_1-AO...August 6 2021.pdf
DOCUMENT ID	c0e0ba1850b5a899cf53c98a267c8075a14dee24
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Completed

Document History

SENT	**08 / 06 / 2021** 14:25:30 UTC-6	Sent for signature to Samuel Lafrenaye Lamontagne (samuel@rebilly.com) and William C Kincaid (wkincaid@darasecurity.com) from wkincaid@darasecurity.com IP: 98.245.212.68
VIEWED	**08 / 06 / 2021** 14:31:23 UTC-6	Viewed by Samuel Lafrenaye Lamontagne (samuel@rebilly.com) IP: 107.159.98.35
SIGNED	**08 / 06 / 2021** 14:33:52 UTC-6	Signed by Samuel Lafrenaye Lamontagne (samuel@rebilly.com) IP: 107.159.98.35
VIEWED	**08 / 06 / 2021** 14:44:31 UTC-6	Viewed by William C Kincaid (wkincaid@darasecurity.com) IP: 98.245.212.68
SIGNED	**08 / 06 / 2021** 14:44:44 UTC-6	Signed by William C Kincaid (wkincaid@darasecurity.com) IP: 98.245.212.68
COMPLETED	**08 / 06 / 2021** 14:44:44 UTC-6	The document has been completed.