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:	Classy, Inc.		DBA (doing business as):	Not Applicable	
Contact Name:	Corey Hall		Title:	Director, Information Security and Platform Operations	
Telephone:	1-619-598-1800		E-mail:	chall@classy.org	
Business Address:	350 Tenth Avenue, Suite 1300		City:	San Diego	
State/Province:	CA	Country:	United States	Zip:	92101
URL:	https://www.classy.org				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Fred Holborn		Title:	Sr. Consultant	
Telephone:	1-303-554-6333		E-mail:	CoalfireSubmission@coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	CO	Country:	United States	Zip:	80021
URL:	https://www.coalfire.com				

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:	Classy Online Fundraising Platform	
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):
☐ 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.*

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:	None	
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:	Not Applicable	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Classy collects payments for donations made to non-profit campaigns on behalf of its customers via ecommerce, payment card-not-present methods. Donation campaign web pages are loaded to the customers' browsers from donation pages hosted in Classy's Fundraising Suite (FRS). The donor's browser performs an asynchronous JavaScript RESTful GET call to the FRS web server to retrieve campaign parameters (customer and campaign ID) and an HTTPS iFrame URL served from Stripe, Inc. or TokenEx, Inc., PCI-validated third-party payments processing service providers. The donor enters their cardholder information consisting of name, PAN, expiry, and card verification values (CVV2, CVC2, CID; hereinafter, referred to as "CVV") into the Stripe or TokenEx iFrame. Payment card information is securely transmitted directly from donor's browser to Stripe or TokenEx via HTTPS/TLS 1.2 with at least AES 128-bit

	encryption. Stripe or TokenEx stores the cardholder information consisting of name, PAN, and expiration date. Stripe or TokenEx returns a token value and CVV to Classy. CVV is stored temporarily in memory only until the transaction completes. Classy stores the returned Stripe and TokenEx token values for recurring donations in an AWS Aurora MySQL relational database system (RDS). Stripe and TokenEx utilize their own secure data vaulting services to store cardholder data (name, PAN, expiration date). For one-time donations, Classy transmits the token value outbound to Stripe or TokenEx. Stripe or TokenEx retrieves the stored credit card information and transmits the payment information to the selected payment processors (Authorize.net, Braintree, WePay, Stripe). The payment processors return the transaction results directly to Classy's Pay Application, which include success/failure code and customer ID. No cardholder data is returned from the payment processors to Classy. For recurring donations, an AWS Lambda function checks for recurring transaction flags stored along with customer information in the AWS Aurora MySQL relational database system (RDS) and when a match is found, the customer ID or transaction token is transmitted outbound directly to the payment processors via the payment processors' APIs. The payment processors return the transaction results directly to Classy's Pay Application. No cardholder data (PAN or SAD) is returned with the payment processor responses or stored by Classy.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	None. All payment flows are described above.

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):
Amazon Web Services (AWS) Cloud Hosting Provider	1	AWS us-east-1 (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)
Not Applicable	Not Applicable	Not Applicable	☐ Yes ☐ No	Not Applicable

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.*	Classy's CDE is entirely hosted in a dedicated Amazon Web Service Virtual Private Cloud (AWS VPC) environment, which is both physically and logically separated from the company's corporate offices and development/testing environments. No direct physical or point-to-point VPN connection exists between the production PCI in-scope AWS environment and the Classy corporate office network or the development testing environment. Classy's CDE is a dedicated AWS VPC with specific AWS Security Groups configured for inbound/outbound traffic. Within Classy's production AWS CDE environment, each system is segmented from other systems with AWS VPC security zones configured with specific rules to allow only traffic necessary between the virtual instances for the application functionality. Technologies utilized by Classy include: AWS Services • Elastic Compute Cloud (EC2): Provides resizable compute capacity in the Cloud. • Virtual Private Cloud (VPC): Provisions a logically isolated section of the AWS Cloud. • CloudFront: Accelerates static and dynamic web content distribution. • Elastic Load Balancers (ELB): Redirects traffic to healthy Amazon EC2 instances for more consistent application performance. • Lambda: Serverless compute service managed by AWS. • Fargate: Serverless compute engine for containers. • Simple Storage Service (Amazon S3): Provides secure and scalable object storage. • Security Groups/Network Access Control Lists (NACLs): Security Groups act as virtual firewalls controls traffic to or from an EC2 instances and NACL controls traffic to or from a subnet based on defined inbound/outbound traffic and defines IP addresses and ports allowed into and out of the VPC. • RDS: Aurora MySQL Relational Database System for storing customer information and recurring payment tokens. • CloudWatch: Collects monitoring and operational data in the form of logs, metrics, and events. • CloudTrail: Enables governance, compliance, operational auditing, and risk auditing. • Inspector: Automated security assessment service. • Network Time Protocol (NTP) for system clock synchronization. Transmission Security

	• HTTPS/TLS 1.2 with AES 128-bit or greater encryption for transmitting CHD to TokenEx or Stripe for tokenization and vaulting • SSHv2 using 2048-bit RSA key pairs with AES 128-bit minimum cipher strength for secure remote access to the CDE Servers AWS Instances • Web-Application Servers for hosting Pay AppInstance. • Bastion Servers to provide secure remote connectivity with multi-factor authentication. Support Systems/Applications • File Integrity Monitoring (FIM) open-source host-based Intrusion Detection System (IDS) file integrity checking, policy monitoring, rootkit detection, and real-time alerting. • External, internal and web application vulnerability scanning. • Host-based IDS monitoring and detection of malicious activity. • Laptops used by Classy's DevOps/administrators to manage/maintain CDE system components hosted on AWS. Tokenization Services • TokenEx • 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 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:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable
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:**
Amazon Web Services	Cloud Hosting Provider
Cloudflare	Web Application Firewall Service
TokenEx	Tokenization Provider
Stripe	Tokenization Provider
CyberSource / Authorize.net	Payment Processor
Braintree	Payment Processor
WePay	Payment Processor
Note: *Requirement 12.8 applies to all entities in this list.*	

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:	Classy Online Fundraising Platform

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 1.3.6 Not Applicable – Classy does not store CHD on any in-scope systems components.
Requirement 2:	☐	☒	☐	Requirement 2.1.1 Not Applicable – Classy does not utilize wireless technologies within or connected to its CDE. Requirement 2.2.3 Not Applicable – Classy does not utilize insecure protocols within its CDE. Requirement 2.6 Not Applicable – Classy is not a shared hosting provider.
Requirement 3:	☐	☒	☐	Requirements 3.1, 3.4.1, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8 Not Applicable – Classy does not store cardholder data on any in-scope systems components.
Requirement 4:	☐	☒	☐	Requirement 4.1.1 Not Applicable – Classy does not utilize wireless technologies within or connected to its CDE.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	Requirements 6.5.7, 6.5.9 Not Applicable – The Classy application uses APIs only. Requirement 6.5.10 Not Applicable – The Classy application does not use cookies or sessions.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Requirement 8.1.3 Not Applicable – No users with CDE access were terminated during the past year.

				Requirement 8.1.5 Not Applicable – Classy does not allow vendors to access its CDE remotely. Requirement 8.5.1 Not Applicable – Classy has no access to customer premises. Requirement 8.7 Not Applicable – Classy does not store cardholder data on any in-scope systems components.
Requirement 9:	☐	☒	☐	Requirements 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.8.1 Not Applicable – Classy does not store CHD on any media. Requirements 9.9, 9.9.1, 9.9.2, 9.9.3 Not Applicable – Classy does not own or manage point-of-sale (POS) devices used for card-present transactions.
Requirement 10:	☐	☒	☐	Requirement 10.2.1 Not Applicable – Classy does not store CHD on any in-scope systems components.
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☒	☐	Requirements A1.1, A1.2, A1.3, A1.4 Not Applicable – Classy is not a shared hosting provider.
Appendix A2:	☐	☒	☐	Requirement A2.1, A2.2, A2.3 Not Applicable – Classy does not own or manage point-of-sale (POS) devices used for card-present transactions.

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:	*10/21/2021*	
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

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *10/21/2021.*

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 *Classy, Inc.* 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 *Not Applicable* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: *Not Applicable* 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
Not Applicable	Not Applicable

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.

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 *Coalfire Systems, Inc.*

Part 3b. Service Provider Attestation

DocuSigned by:
Corey Hall
417A5139219646B...

Signature of Service Provider Executive Officer ↑	*Date:* 10/21/2021
Service Provider Executive Officer Name: Corey Hall	*Title:* Director, Information Security and Platform Operations

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Conducted PCI DSS v3.2.1 assessment and documented compliance results in a Report on Compliance (ROC) and associated Attestation of Compliance (AOC).

Fred Holborn

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 10/21/2021
Duly Authorized Officer Name: Fred Holborn	*QSA Company:* Coalfire Systems, Inc.

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 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	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐