PCI DSS COMPLIANCE VALIDATION

The Payment Card Industry (PCI) Security Standards Council (SSC) is an open global forum founded by a consortium of the major card brands. The PCI SSC created and maintains the PCI Data Security Standard (DSS) which encourages and enhances cardholder data security and facilitates the broad adoption of consistent data security measures globally. The PCI DSS Requirements and Security Assessment Procedures set forth 12 PCI DSS requirements, and denes compliance testing procedures, to form a common security assessment tool. The current version of the PCI DSS can be found at www.pcisecuritystandards.org.

This document confirms that Schellman & Company, LLC, a certified Qualified Security Assessor (QSA) Company, utilized these procedures to conduct an onsite assessment for this Service Provider and validated its compliance with the applicable sections of the PCI DSS version 3.2.1.

SERVICE PROVIDER:	**Chargify, LLC**
SERVICE PROVIDER CATEGORY:	**Level 1 Service Provider**
SERVICES COVERED BY ASSESSMENT:	**Chargify Recurring Billing Application**
FACILITIES COVERED BY ASSESSMENT:	**AWS Facilities Previously Assessed Under Separate AOC**
REPORT ON COMPLIANCE VALIDATION DATE:	**December 06, 2019**

Conditions & Limitations

1. This document is supplemental to the compliance validation services provided by Schellman & Company, LLC and is not a replacement for the official PCI Security Standards Council's templates and forms which have been approved by the payment brands.
2. The Service Provider has a perpetual responsibility to maintain compliance with the PCI DSS. Schellman & Company, LLC's Report on Compliance opines on the Service Provider's compliance with the PCI DSS as of a date in time and should not be construed as evidence of compliance for any date, or period of time, other than the Report on Compliance Validation Date.
3. Onsite PCI DSS compliance assessments are not designed to detect or prevent criminal activity or other acts that may result in a breach of cardholder data. PCI DSS compliance validation should not be construed as a guarantee or assurance that a Service Provider is unsusceptible to cardholder data breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. Schellman & Company, LLC expressly disclaims any representations and warranties, including without limitation, the implied warranties of merchantability and fitness for a particular purpose.

schellman