Subject: Supplement to Lighthouse Transaction Manager® (LTM®) Service Agreement.

Background:

- PCI DSS Requirement 12.8.5 requires that merchants maintain information about which PCI DSS requirements are managed by service providers.

- PCI DSS Requirement 12.9 requires that service providers acknowledge in writing that they are responsible for the security of cardholder data they process, store, or transmit on behalf of merchants.

Here are the verbatim requirements:

- 12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

- 12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

This SUPPLEMENT TO LIGHTHOUSE TRANSACTION MANAGER® (LTM®) SERVICE AGREEMENT ("Supplement") specifies PCI DSS Roles and Responsibilities for both SHIFT4 and its CLIENTs. The supplemental information contained herein does not supersede any statement or section of a previously executed LTM SERVICE AGREEMENT with Shift4 Payments, LLC, but rather it provides more detailed information regarding PCI DSS Roles and Responsibilities for both entities.

Shift4 General Roles and Responsibilities

1. Shift4 maintains its status as a PCI DSS validated Level 1 Service Provider and its listing as a Visa Agent/Merchant Servicer on Visa's Global Registry of Service Providers (http://www.visa.com/splisting/searchGrsp.do).

2. Shift4 undergoes an annual PCI DSS onsite ROC assessment by a Qualified Security Assessor Company.

3. As part of its recurring compliance related tasks, Shift4 performs monthly ASV vulnerability scans plus additional internal and external security vulnerability scans with a different scanning vendor.

4. Shift4's LTM software as a service will process, store, and transmit Client's cardholder data in compliance with all PCI DSS security controls.

Client's General Roles and Responsibilities

1. The Client is responsible to maintain its cardholder data environment in compliance with the PCI DSS.

2. The Client is responsible to complete the relevant Self-Assessment Questionnaire and Attestation of Compliance and file them with its acquiring bank.

3. The Client is responsible to maintain its cardholder data environment in a PCI DSS compliant state so long as Shift4 software is installed and operating on its premise.

Shift4's and Client's Specific PCI DSS Roles and Responsibilities

Build and Maintain a Secure Network and Secure Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

- Shift4 performs no specific Requirement 1 security controls on behalf of the client.
- Client is responsible to protect its cardholder data environment and all Shift4 installed software behind firewalls.

Requirement 2: Do not use vendor-supplied defaults for systems passwords and other security parameters.

- Shift4 performs no specific Requirement 2 security controls on behalf of the client.
- Client is responsible to use supported operating systems in its cardholder data environment and where Shift4 software is installed and operating and maintain them in accordance with Requirement 2.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

- Shift4 stores Client's cardholder data in compliance with all Requirement 3 security controls.
- Client is responsible to protect any stored cardholder data in compliance with all Requirement 3 security controls.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

- Shift4 transmits Client's cardholder data in accordance with all Requirement 4 security controls so long as the Universal Transaction Gateway® (UTG®) is maintained in a PCI DSS compliant state by Client on Client's premise.
- Client is responsible to ensure the UTG is protected behind firewall(s), maintained in a PCI DSS compliant state, and configured in accordance with the UTG PA-DSS Implementation Guide.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.

- Shift4 performs no specific Requirement 5 security controls on behalf of the client.
- Client is responsible to protect all systems against malware in accordance with all Requirement 5 security controls.

Requirement 6: Develop and maintain secure systems and applications.

- Shift4 develops and deploys LTM software as a service in compliance with all Requirement 6 security controls.
- Shift4 develops and deploys payment applications for Client as part of the LTM software as a service in accordance with PCI DSS and PA-DSS.
- All Shift4 payment applications are validated under PCI PA-DSS and appear on the PCI Security Standards Council's validated payment application list (https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php).
- Client is responsible to develop and maintain secure systems for its cardholder data environment and where Shift4 software is installed and operating, with particular emphasis on Requirement 6.2.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know.

- Shift4 performs no specific Requirement 7 security controls on behalf of the client.
- Client is responsible for all Requirement 7 security controls.

Requirement 8: Identify and authenticate access to system components.

- Shift4 performs no specific Requirement 8 security controls on behalf of the client.
- Client is responsible for all Requirement 8 security controls.

Requirement 9: Restrict physical access to cardholder data.

- Shift4 performs no specific Requirement 9 security controls on behalf of the client.
- Client is responsible for all Requirement 9 security controls.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

- Shift4 performs no specific Requirement 10 security controls on behalf of the client.
- Client is responsible for all Requirement 10 security controls.

Requirement 11: Regularly test security systems and processes.

- Shift4 performs no specific Requirement 11 security controls on behalf of the client.
- Client is responsible for all Requirement 11 security controls.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

- Shift4 performs no specific Requirement 12 security controls on behalf of the client.
- Client is responsible for all Requirement 12 security controls.