CARDHOLDER DATA SECURITY

1. For the purposes of this addendum, the following terms will have the meaning ascribed to them herein.
   a. “Cardholder Data” shall mean, at a minimum, the full Primary Account Number (PAN). Cardholder Data may also consist in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code;
   b. “Subcontractors” means all parties, if any with which Provider contracts, directly or indirectly, in order to perform its obligations under the Agreement.

2. Provider agrees, on behalf of itself and each of its Subcontractors, that it shall be responsible for the security of any cardholder data possessed or otherwise stored, processed or transmitted on behalf of the customer, or to the extent that Provider could impact the security of the customer’s cardholder data environment. Provider shall use cardholder data only for assisting cardholders in completing a transaction, supporting a loyalty card program, providing fraud control services, or for other uses specifically required by law.

3. Provider, on behalf of itself and all subcontractors, agrees (a) to provide University a copy of mutually acceptable PCI DSS compliance documentation containing information about which PCI DSS requirements are managed by the provider, which PCI DSS requirements should be managed by the University, and which PCI DSS requirements have a shared responsibility; (b) that the PCI DSS compliance documentation will be updated and a copy provided to the University annually; (c) that University will have the right to review the audit criteria for any such documentation; (d) that it will notify the University at least 60 days prior to any substantial change to the processing environment that may impact the University; and (e) that it will establish and maintain all application and system logs under its domain and provide to University a copy of all logs for any period up to the full PCI DSS retention period if so requested.

4. Provider will immediately notify University Accounts Receivable Services by sending an e-mail to pmtcard@umn.edu if Provider learns that it or any of its subcontractors are no longer PCI DSS compliant, and will immediately provide the University the steps being taken to remediate the non-compliant status. In no event shall Provider’s notification to the University be later than seven (7) calendar days after Provider learns of the non-compliant condition. Failure to maintain PCI DSS compliance shall be a breach of contract and the University may, at its sole discretion, terminate this Agreement if Provider does not become compliant within thirty (30) days, [with any prepaid amounts refunded to University on a pro-rata basis].

5. In the event of a breach or intrusion, or otherwise unauthorized access to cardholder data or cryptographic keys stored at or for Provider, Provider shall immediately notify the University Information Security Incident Response Team by calling (612) 301-4357 or sending an e-mail to security@umn.edu stating that this incident involves payment card cardholder data. Provider shall provide appropriate payment card companies, acquiring financial institutions, and their respective designees access to the Provider's facilities and all pertinent records to conduct a review of the Provider's compliance with the PCI DSS requirements. Provider will cooperate with representatives or agents of the payment card industry and/or University in conducting a thorough security review of Provider’s operations, systems, records, procedures, rules and practices in the event of a security intrusion in order to validate Provider’s compliance with PCI DSS. Provider acknowledges any/all costs related to breach or intrusion or unauthorized access to cardholder data entrusted to Provider deemed to be the fault of Provider shall be the liability of Provider. Provider agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify and hold harmless University and its officers and employees from and against any claims, damages or other harm related to such breach.

6. Provider shall have a business continuity program which conforms to PCI DSS to protect cardholder data in the event of a major disruption in its operations or in the event of any other disaster or system failure which may occur to Provider’s operations.

7. Provider shall respond in a timely manner and fully to those portions of the PCI DSS Annual Self-Assessment Questionnaire or any other documentation demonstrating compliance sent to it by the University.

8. Provider shall securely delete and provide evidence of destruction of client cardholder data in the event this Agreement terminates or expires. If secured deletion is not possible, Provider shall continue to safeguard cardholder data in the event this Agreement terminates or expires.

9. Provider shall indemnify, defend and hold the University and its regents, faculty members, students, employees, agents and contractors harmless from actions, suits, claims, losses, costs, judgments, fines, penalties (including any fines or penalties imposed on the University by Payment Card Companies or their acquiring banks), and expenses (including reasonable attorneys' and investigative fees), arising out of Provider's failure to comply with the representations and warranties in this Agreement.