Indiana University Payment Card Merchant Agreement

This Merchant Agreement (the “Agreement”), executed on the date stated below, which includes any schedule or addendum to this Agreement, all of which are incorporated herein by reference, is entered into between Indiana University, Office of the Treasurer, Treasury Operations (referred to as “Indiana University”, “IU”, “Office of the Treasurer”, “Treasury Operations”, “Treasury”, “we”, “us”, or “our”) and you, the undersigned Indiana University Department (referred to as “Merchant”, “Department”, “you”, or “your”). Treasury will administer the process so that you will be capable of accepting payment cards. Along with this privilege, come required responsibilities. In the event of non-compliance, Treasury reserves the right to revoke the ability to accept payment cards until which time compliance is achieved. Treasury will deposit funds and deduct fees to the IU general ledger system. That you want to receive these services, we, Indiana University, Office of the Treasurer, and you, the department, agree to the following terms and conditions:

1. Merchant’s Acceptance of Payment Instruments.

1.1 Certain Payment Acceptance Policies and Prohibitions.

(a) Each Transaction must be evidenced by its own Transaction Receipt completed in accordance with Payment Brand Rules.

(b) Merchant shall not require the Customer to pay the fees payable by Merchant under this Agreement.

(c) Merchant shall never issue Refunds for Transactions by cash or a cash equivalent (e.g. check) unless specifically approved by Treasury.

(d) Unless permitted by the Payment Brand Rules, Merchant shall not engage in any practice that unfavorably discriminates against or provides unequal treatment of any Payment Brand relative to any other Payment Brand.

(e) Merchant may be allowed to set a minimum dollar amount which Merchant refuses to honor otherwise valid Payment Instruments. However, Merchant must have prior approval from Treasury to do so.

(f) Merchant shall examine each Payment Instrument physically presented at the point of sale to determine that the Payment Instrument presented is valid and has not expired. Merchant shall exercise reasonable diligence to determine that the authorized signature on any Payment Instrument physically presented at the point of sale corresponds to the Customer’s signature on the Transaction Receipt.

(g) With respect to any Transaction for which a Customer is not physically present at the point of sale, such as in any on-line, mail, telephone, pre-authorized or recurring Transaction (e-mail or unsecured fax are not secure formats), Merchant must (i) have notified Treasury on its Application, or otherwise obtained Treasury’s prior written approval, of Merchant’s intention to conduct such Transactions; and (ii) have appropriate procedures in place to ensure that each Transaction is made to a purchaser who actually is a Customer (i.e., mail-in form with card information and signature). Merchant acknowledges that under certain Payment Brand Rules, Merchant cannot rebut a Chargeback where the Customer disputes making the purchase and Merchant does not have an electronic record (e.g., “swiping” or “tapping” a Payment Instrument) or physical imprint of the Payment Instrument.

(h) With respect to any Transaction processed via IUPayPlus, Merchant will not collect payment information from Customer and then submit information via the IUPayPlus Payment Page. All IUPayPlus payments must be entered directly by Customer on the IUPayPlus Payment Pages. The CVV2 or CVC2 number is a required item. Collection and/or storage of this number is prohibited by Visa/MC Rules and Regulations.

(i) Merchant agrees to accept all categories of Payment Instruments (i.e., debit cards, Visa, MasterCard, Discover, American Express, JCB).

(j) Merchant shall not split a single Transaction into two or more Transactions to avoid or circumvent authorization limits or monitoring programs.

(k) Merchant must obtain prior approval for any form, document, or application, whether paper or electronic, which includes the Customer’s Payment Instrument account number, expiration date, or any other account data.

(l) Merchant shall not add any tax or surcharge to Transactions, unless applicable law expressly requires a Merchant be permitted to impose the tax or surcharge. If any tax or surcharge amount is allowed, such amount shall be included in the Transaction amount and shall not be collected separately (see Section 12.1 Taxes).
(m) Merchant shall not request or use a Payment Instrument account number for any purpose except as payment for its goods or services, unless required by the Payment Brand Rules in order to support specific services offered by the Payment Brands.

(n) Merchant should maintain transaction activity monthly to remain active and be considered an open account.

1.2 Payment Brand Rules. Merchant agrees to comply with (a) all Payment Brand Rules as may be applicable to Merchant and in effect from time to time; and (b) such other procedures as Treasury may from time to time prescribe for the creation or transmission of Transaction Data.

1.3 Requirements for Certain Transactions. As to all Transactions, Merchant represents and warrants that, to the best of its knowledge:

(a) The Transaction Data (i) represents a payment for or Refund of a bona fide sale or lease of the goods, services, or both, which Merchant has provided in the ordinary course of business, as represented in its Application; and (ii) is not submitted on behalf of a third party.
(b) The Transaction Data represents an obligation of the Customer for the amount of the Transaction.
(c) The Transaction is not for any purpose other than payment for the current Transaction. The Transaction does not represent the collection of a dishonored check or the collection or refinancing of an existing debt. The Transaction does not represent payment for a previous Transaction or charge incurred at the Merchant or a Transaction that was previously charged back by the Customer, irrespective of Customer consent or approval.
(d) Merchants that collect prepayment must advise the Customer (i) that payment is being made in advance of the shipment or provision of goods or services; and (ii) the time when shipment or provision of the goods or services is expected.
(e) The Transaction Data is free from any material alteration not authorized by the Customer.
(f) The amount charged for the Transaction is not subject to any dispute, setoff, or counterclaim.
(g) Merchant has not disbursed or advanced any cash to the Customer or itself or to any of its representatives, agents, or employees in connection with the Transaction, nor has Merchant accepted payment for effecting credits to a Customer.
(h) The goods or services related to each Transaction are Merchant’s property or Merchant has the legal right to sell them.
(i) Merchant has made no representation or agreement for the issuance of Refunds except as stated in Merchant’s Refund Policy, which has been previously submitted to Treasury in writing as provided in Section 3, and which is available to the Customer.
(j) Any Transaction submitted to Processor to credit a Customer’s account represents a Refund for a Transaction previously submitted to Processor.
(k) Merchant has no knowledge or notice of information that would lead Merchant to believe that the enforceability or collectability of the Transaction is in any manner impaired. Merchant has originated the Transaction and Transaction Data in compliance with this Agreement, applicable laws and all applicable Payment Brand Rules.
(l) Unless specifically stated in its Application or otherwise approved in writing by Treasury in advance, Merchant shall not accept Payment Instruments in connection with installment plans. If the Customer pays in installments or on a deferred payment plan, as previously approved by Treasury, a Transaction Data record has been prepared separately for each installment transaction or deferred payment on the dates the Customer agreed to be charged. All installments and deferred payments, whether or not they have been submitted to Processor for processing, shall be deemed to be a part of the original Transaction.
(m) Merchant has not submitted any Transaction that Merchant knows or should have known to be either fraudulent, illegal, damaging to the Payment Brand(s), not authorized by the Customer or otherwise in violation of any provision of this Agreement, applicable law, or Payment Brand Rules.
(n) For recurring Transactions, Merchant must (i) obtain the Customer’s consent to periodically charge the Customer on a recurring basis for the goods or services purchased, (ii) retain this permission for the duration of the recurring services and provide it upon request to Treasury, Processor or the issuing bank of the Customer’s Payment Instrument; and (iii) retain written documentation specifying the frequency of the recurring charge and the duration of time during which such charges may be made. Merchant shall not submit any recurring transaction after receiving: (i) a cancellation notice from the Customer, or (ii) notice from Processor or any Payment Brand (via
authorization code or otherwise) that the Payment Instrument is not to be honored. Merchant shall include in its Transaction Data the electronic indicator that the Transaction is a recurring Transaction.

2. **Authorizations.** Merchant is required to obtain an authorization code through Processor, in accordance with this Agreement, for each Transaction. Merchant acknowledges that authorization of a transaction indicates that the Payment Instrument (a) contains a valid account number; and (b) has an available credit balance sufficient for the amount of the Transaction; but, it does not constitute a representation from Processor, a Payment Brand, or a card issuing bank that a particular Transaction is in fact a valid or undisputed Transaction entered into by the actual Customer. Processor reserves the right to refuse to process any Transaction Data presented by Merchant unless it includes a proper authorization.

3. **Refund and Adjustment Policies and Procedures; Privacy Policies.**

3.1 **Refund Policy.** Merchant is required to maintain a written Refund Policy and to disclose such Refund Policy to Treasury and Customers. Any material change in Merchant’s Refund Policy must be submitted to Treasury, in writing, not less than 14 days prior to the effective date of such change. Processor reserves the right to refuse to process any Transactions made subject to a revised Refund Policy of which Processor has not been notified in advance. To the extent that Merchant operates an electronic commerce website through which Transaction Data is generated, Merchant must include its Refund Policy on the website in accordance with Payment Brand Rules.

3.2 **Procedure for Refund Transactions.** If, under Merchant’s Refund Policy, Merchant allows a Refund, Merchant shall prepare and deliver to Processor Transaction Data reflecting any such Refund within three (3) days of approving the Customer’s request for such Refund. The amount of a Refund cannot exceed the amount shown as the total on the original Transaction Data except by the exact amount required to reimburse the Customer for shipping charges that the Customer paid to return merchandise. Merchant shall not accept any payment from a Customer as consideration for issuing a Refund. Merchant shall not give cash (or cash equivalent) refunds to a Customer in connection with a Transaction, unless required by law or permitted by the Payment Brand Rules.

4. **Settlement.**

4.1 **Submission of Transaction Data.** Failure to transmit Transaction Data to Processor within one (1) business day following the day that such Transaction originated could result in higher interchange fees and other costs, as well as increased Chargebacks. Unless Merchant has notified Treasury on its Application or Treasury has otherwise agreed in writing in advance, Merchant shall not submit Transactions for processing until (a) the Transaction is completed; (b) the goods are delivered or shipped; (c) the services are performed; or (d) Merchant has obtained the Customer’s consent for a recurring Transaction. Processor may from time to time contact Customers to verify that they received goods or services for which Transactions have not been submitted. Processor reserves the right to refuse to process any Transaction Data presented by Merchant if Processor reasonably believes that the Transaction may be uncollectible from the Customer or was prepared in violation of any provision of this Agreement, applicable law, or the Payment Brand Rules. For all Transactions, Processor will submit Merchant’s Transaction Data to the applicable Payment Brands.

4.2 **Merchant’s Settlement Account.** The daily sales will automatically settle into the appropriate bank account designated by Treasury. This information is automatically fed into Indiana University’s Kuali Financial System (KFS). Income and the associated processing fees are placed into a valid IU KFS account number(s). The posting will occur Sunday through Friday. Any changes to the KFS account number(s) must be requested by the Fiscal Officer for that account via Treasury’s Credit Card General Ledger Accounting Change Form.

5. **Accounting and Reconciling.**

5.1 **Accounting.** Processor will supply a detailed statement reflecting the activity of Merchant’s account(s) by online access and Merchant shall ensure that any online access to such statements is secure. If Merchant believes any adjustments should be made with respect to Merchant’s Settlement Account, Merchant must notify Treasury via the online Treasury Research System (https://www.indiana.edu/~iutreas/treasuryresearch/request_form.html)
in writing within 60 days after any such adjustment is or should have been affected. Failure could result in loss of funds.

5.2 Reconciling. It is the responsibility of the Merchant to reconcile the settlement amount in the general ledger (via the Indiana University Information Environment IUIE) to the credit card receipts and the Merchant Billing Statement provided by Processor. Reconciling must be done on a daily basis. Any discrepancies are the responsibility of the Merchant to reconcile. If Merchant is unable to reconcile any discrepancy, Merchant should notify Treasury, Payment Card Services immediately.

6. Retrieval (Copy) Requests. In order to comply with Retrieval Requests, Merchant shall store and retain Transaction Data and Transaction Receipts in compliance with the Payment Brand Rules, including any time frames set forth therein. Within seven (7) days (or such shorter time as the Payment Brand Rules may require) of Processor sending Merchant a Retrieval Request, Merchant must provide to Processor, (a) written resolution of Merchant’s investigation of such Retrieval Request; and (b) legible copies of any supporting documentation requested or required by the Retrieval Request. Merchant acknowledges that failure to fulfill a Retrieval Request timely and in accordance with Payment Brand Rules may result in an irreversible Chargeback.

7. Chargebacks.
7.1 Chargeback Reasons. Merchant has full liability for all Chargebacks. Following are some of the most common reasons for Chargebacks:
(a) Merchant fails to issue a Refund to a Customer upon the return or non-delivery of goods or services;
(b) A required authorization/approval code was not obtained;
(c) The Transaction Data was prepared incorrectly or fraudulently;
(d) Processor did not receive Merchant’s response to a Retrieval Request in accordance with Section 6;
(e) The Customer disputes the Transaction or the authenticity of the signature on the Transaction Receipt, or claims that the Transaction is subject to a set-off, defense, or counterclaim;
(f) The Customer refuses to make payment for a Transaction because, in the Customer’s opinion, a claim or complaint has not been resolved or has been resolved in an unsatisfactory manner; or
(g) The credit or debit card comprising the Payment Instrument was not actually presented at the time of the Transaction or Merchant failed to obtain an electronic record or physical imprint of such Payment Instrument, and the Customer denies making the purchase.

7.2 Response to Chargebacks. If Merchant has reason to dispute or respond to a chargeback, then Merchant must do so by the date provided on the applicable Chargeback notice. Processor will not investigate or attempt to obtain a reversal or other adjustment to any Chargeback if Merchant has not timely responded to the notice.

7.3 Excessive Chargebacks. If Merchant is receiving an excessive amount of Chargebacks, as determined by the Payment Brands from time to time, in addition to Treasury’s other remedies under this Agreement, Treasury may take one or more of the following actions: (a) review Merchant’s internal procedures relating to acceptance of Payment Instruments and notify Merchant of new procedures Merchant should adopt in order to avoid future Chargebacks; (b) notify Merchant of a new rate Processor will charge to process Merchant’s Chargebacks. Merchant also agrees to pay any and all penalties, fees, fines, and costs assessed against Merchant, Processor, and/or Member relating to Merchant’s violation of this Agreement or the Payment Brand Rules with respect to Merchant’s acceptance of Payment Instruments, its Transactions, or with respect to excessive Chargebacks under this Section.

7.4 Claims of Customers. Following a Chargeback, Merchant may resubmit applicable Transaction Data for a second presentment, but only in accordance with Payment Brand Rules. To the extent Processor has paid or may be called upon to pay a Chargeback or Refund for or on the account of a Customer and Merchant does not reimburse Processor as provided in this Agreement, then for the purpose of Processor obtaining reimbursement of such sums paid or anticipated to be paid, Processor has all of the rights and remedies of such Customer under applicable federal, state, or local laws and Merchant authorizes Processor to assert any and all such claims in its own name for and on behalf of any such Customer individually or all such Customers as a class.
8. **Display of Payment Brand Marks.** Merchant is prohibited from using the Payment Brand Marks, as defined below (sometimes referred to herein as “Marks”), other than as expressly authorized by Treasury in writing or by the Payment Brands. Additionally, Merchant shall not use the Payment Brand Marks other than to display decals, signage, advertising, and other forms depicting the Payment Brand Marks that are provided to Merchant (a) by the Payment Brands; (b) by Treasury pursuant to this Agreement; or (c) as otherwise approved in writing by Treasury. Merchant may use the Payment Brand Marks only to promote the services covered by the Marks by using them on decals, indoor and outdoor signs, advertising materials, and marketing materials; provided, that all such uses by Merchant must be approved by Treasury and consistent with Payment Brand Rules. Merchant shall not use the Payment Brand Marks in any way that Customers could believe that the goods or services offered by Merchant are sponsored, endorsed, or guaranteed by the owners of the Payment Brand Marks. Merchant recognizes that it has no ownership rights in the Payment Brand Marks. Merchant shall not assign the rights to use the Payment Brand marks to any third party. Merchant’s right to use the Payment Brand Marks hereunder terminates with the termination of this Agreement.

9. **Fees.** Merchant shall pay all applicable fees for all Transactions, which shall be calculated and payable pursuant to this Agreement. Fees shall be deducted from the expense account specified by the first week of the following month. The expense account in this Merchant Agreement must have sufficient funds to allow an orderly billing process. It is the Merchant’s responsibility to verify the fee charged to the General Ledger.

10. **Termination.**
10.1 **Term.** This Agreement takes effect upon Treasury’s signature and continues for one (1) year from such date. The Agreement will be subject to renewal for one-year term, subject to mutual agreement by the parties. Requests to activate/deactivate/suspend a merchant account must be received in writing from Fiscal Officer via pmtcards@iu.edu.

10.2 **Other Events.** In addition to the remedies above and any rights Treasury may have under this Agreement, Treasury may suspend the processing of some or all of Merchant’s Transactions upon: (a) failure to comply with all rules, policies, PCI DSS; (b) receipt by Processor of notice that a Payment Brand intends to impose any fine or penalty as a result of excessive Chargebacks or Merchant’s acts or omissions; or (c) receipt by Processor of objections or concerns expressed by a Payment Brand which render Processor’s continued processing of Merchant’s Transactions unduly burdensome, impractical, or risky.

10.4 **Account Activity After Termination.** The provisions governing processing and settlement of Transactions, all related adjustments, fees and other amounts due from Merchant, and the resolution of any related Chargebacks, disputes, or other issues involving Transactions, will continue to apply even after termination of this Agreement, with respect to all Transactions made prior to such termination or after such termination. After termination of this Agreement for any reason whatsoever, Merchant shall continue to bear total responsibility for all Chargebacks, fees, fines, assessments, credits, and adjustments resulting from Transactions processed pursuant to this Agreement and all other amounts then due or which thereafter may become due to Processor under this Agreement or which may be due to Processor before or after such termination to either Processor or Bank. If Merchant submits Transaction Data to Processor after the date of termination, Processor may, at its sole discretion process such Transaction Data in accordance with and subject to all of the terms of this Agreement.

11. **Payment Card Industry Compliance.** Merchant acknowledges and understands the importance of compliance with the Security Standards, such as those relating to the storage and disclosure of Transaction Data and Payment Instrument Information. Therefore, Merchant shall exercise reasonable care to prevent disclosure or use of Payment Instrument Information, other than (a) to Merchant’s agents and contractors for the purpose of assisting Merchant in completing a Transaction; (b) to the applicable Payment Brand; or (c) as specifically required by law. Furthermore, Merchant acknowledges and understands that its use of any fraud mitigation or security enhancement solution (e.g. an encryption product or service), whether provided to Merchant by Treasury or a
third party, in no way limits Merchant’s obligation to comply with the Security Standards or Merchant’s liabilities set forth in this Agreement.

Merchant is allowed by the Payment Brand Rules to store only certain Payment Instrument Information (currently limited to the Customer’s name, Payment Instrument truncated account number, and expiration date) and is prohibited from storing additional Payment instrument information, including, without limitation, any security code data, such as CVV2, CVV2, and PIN data, and any magnetic stripe track data. Merchant shall store all media containing Payment Instrument Information in an unreadable format wherever it is stored and in an area limited to selected personnel on a “need to know” basis only. (Secure environments include locked drawers, file cabinets in a locked office, and safes.) Prior to either party discarding any material containing Payment Instrument Information, the party will render the account numbers unreadable in accordance with the requirements of the Security Standards. If at any time Merchant determines or suspects that Payment Instrument Information has been compromised Merchant must notify Treasury immediately and assist in providing notification to such parties as may be required by law or Payment Brand Rules, or as Processor otherwise reasonably deems necessary. Merchant information may be shared by Processor with its affiliates and with the Payment Brands subject to the provisions of this Agreement and Payment Brand Rules.

Merchant agrees to comply with all Security Standards. Merchant agrees that any person involved in the acceptance, processing, or storage of credit card data will complete the mandatory Security Awareness Education (SAE) online training prior to processing payments, and then annually, thereafter. Full time staff must complete face to face Revenue Processing training every two years. Part time staff much complete the online Revenue Processing Tutorial every two years. Merchant agrees it is the Fiscal Officer’s responsibility to ensure that all compliance training is complete. On an annual basis, by December 31st, Merchant will complete a PCI DSS Self Assessment Questionnaire (SAQ) to maintain compliance with the Payment Card Industry Data Security Standards. All Merchants must complete this assessment on an annual basis to evaluate Merchant’s payment card processes so that remediation can be taken on procedures which are out of compliance. Merchant further agrees to provide Treasury, upon its request, with such tests, scans, and assessments of Merchant’s compliance with Security Standards as may from time to time be required by the Payment Brands.

Merchant must notify Treasury of its use of any Service Provider and Treasury must provide approval to use Service Provider prior to Agreement; and, to the extent required by each Payment Brand all Service Providers must be (i) compliant with all Security Standards applicable to Service Providers; and (ii) registered with and/or recognized by such Payment Brand(s) as being so compliant. Merchant agrees to exercise due diligence to ensure that all Service providers, and any other agents, business partners, contractors, or subcontractors with access to Merchant’s Payment Instrument Information, shall be (i) compliant with all Security Standards applicable to such Payment Applications or software; and (ii) registered with and/or recognized by such Payment Brand(s) as being so compliant.

Merchant understands that failure to comply with the Payment Brand Rules, including the Security Standards, or the compromise of any Payment Instrument Information, may result in fees, fines, and/or penalties by the Payment Brands in addition to the suspension or closure of the merchant account. Merchant is responsible for paying all such fees, fines, and/or penalties assessed. By executing this Agreement, Merchant represents that in the event of suspension of business operations, Merchant shall not sell, transfer, or disclose to third parties any materials that contain Transaction Data to Processor or provide Processor with acceptable proof of its destruction.

12. Miscellaneous.
12.1 Taxes. Depending on the circumstances, Indiana University must collect or pay sales tax. It is the responsibility of Merchant to consult with FMS Tax Department to determine if Merchant must collect or pay sales tax, and to ensure Merchant is collecting or paying appropriate taxes on taxable items.
12.2 Account Set-Up and Support.
(a) Merchant must have prior approval from Revenue Producing Activity Committee (RPAC) to process revenue per Indiana University policy VI-121.
(b) After RPAC approval, and upon receipt of the signed completed Departmental Request to Process Payment Cards, Treasury will proceed to create a merchant account with Processor. Merchant will be notified once the account is activated and ready for transaction processing.
(c) Any terminal equipment must be obtained, programmed, and installed by Treasury. Equipment obtained by Treasury is PCI DSS compliant. Merchant must keep equipment in reasonable working order and no terminal is to be exchanged or removed without permission from Treasury. Terminals must be located in a secure environment with limited physical access.
(d) Treasury will provide basic transaction processing training on all systems used to accept payment cards, transaction security, and the settlement process.
(e) Merchant should contact Vantiv Terminal Support at 866-622-2390 for any concerns with terminal function and processing. Treasury will provide merchant support via telephone and/or email during normal business hours (Monday thru Friday, 8am-5pm). Treasury will also act as a liaison to Vantiv in the event concerns are not resolved.
(f) Merchant must retain all payment card documentation for no less than 180 days and no longer than two (2) years.
(g) Merchant’s payment card account is for the explicit use of the Merchant it is assigned to. Merchant will not allow their payment card account access (i.e., terminal, IU PayPlus, etc.) to be used by any other department, person, or entity. Merchant’s account is subject to closure if found in violation.
Signature Page

This Agreement shall not become effective until accepted by Treasury and will remain in full force until terminated by either party by giving written notice to the other party. This Agreement must be re-certified annually by current Fiscal Officer.

I understand the contents, terms, and conditions of this Merchant Agreement. By signing below I agree to abide by all rules and regulations stated here within. Upon Treasury’s approval, a copy of the Merchant Agreement will be uploaded to Department’s merchant folder on Treasury’s SharePoint site.

Please supply KFS General Ledger accounts for this Merchant payment activity. (To update GL information at a later date, please refer to Section 4.2 of Merchant Agreement)

IU KFS Account for Deposits/Income: ______________ Object Code: ____________
IU KFS Account for Fees/Expense: _________________ Object Code: ____________

Please sign and upload to Department’s assigned merchant folder on Treasury’s SharePoint site: https://www.sharepoint.iu.edu/sites/revenue/creditcards/_layouts/viewlsts.aspx

Fiscal Officer (print): ____________________________ Fiscal Officer (print): _________________________
Phone: _______________________________________
Email: ________________________________________
Signature: _____________________________________
Date: _________________________________________

FOR TREASURY USE ONLY

Merchant Name: _________________________________
Merchant Number: ______________________________
Credit Card Processing Type: _____________________
Treasury Approval (print): ________________________
Signature: _____________________________________
Date: _________________________________________
Addendum A.

Definitions.
“Application” means merchant application in the form of: (i) Departmental Request to Process Payment Cards; or (ii) Department Request to Process via IUPayPlus.
“Chargeback” means a reversal of a Transaction Merchant previously presented to Processor pursuant to payment Brand Rules.
“Customer” means the person or entity to whom a Payment Instrument is issued or who is otherwise authorized to use Payment Instrument.
“Data Compromise Event” means an occurrence that results, or could result, directly or indirectly, in the unauthorized access to or disclosure of Transaction Data and/or Payment Instrument Information.
“Effective Date” means the date the Agreement takes effect pursuant to Section 10.0.
“Merchant” means any Indiana University Department accepting payment cards.
“Member” means Bank or other entity providing sponsorship to Processor as required by all applicable Payment Brands. Merchant’s acceptance of Payment Brand products is extended by the Member.
“Payment Application” means a third party application used by Merchant that is involved in the authorization or settlement of Transaction Data.
“Payment Brand” means any payment method provider whose payment method is accepted by Processor for processing, including, without limitation, Visa Inc., MasterCard International, Inc., Discover Financial Services, LLC, and other credit and debit card providers, debit network providers, gift card, and other stored value and loyalty program providers. Payment Brand also includes the Payment Card Industry Security Standards Council.
“Payment Brand Rules” means all bylaws, rules, programs, and regulations, as they exist from time to time, of the Payment Brands.
“Payment Instrument” or “Payment Card” means an account, or evidence of an account, authorized and established between a Customer and a Payment Brand, or representatives or members of a Payment Brand that Merchant accepts from Customers as payment for a good or service. Payment Instruments include credit and debit cards.
“Payment Instrument Information” means information related to a Customer or the Customer’s Payment Instrument, that is obtained by Merchant from the Customer’s Payment Instrument, or from the Customer in connection with his or her use of a Payment Instrument (e.g., a security code, a PIN number, credit limits, account balances, or the customer’s zip code when provided as part of an address verification system). Without limiting the foregoing, such information may include a the Payment Instrument account number and expiration date, the Customer’s name or date of birth, PIN data, security code data (such as CVV2 and CVC2), and any data read, scanned, imprinted, or otherwise stored thereon. For the avoidance of doubt, the data elements that constitute Payment Instrument Information shall be treated according to their corresponding meanings as “cardholder data” and “sensitive authentication data” as such terms are used in the then current PCI DSS.
“Processor” means Vantiv.
“Refund” means any refund or credit issued for any reason, including, without limitation, for a return of merchandise or cancellation of services, and any adjustment of a Transaction.
“Refund Policy” means a written policy with regards to Refunds.
“Retrieval Request” means a request for information by a Customer or Payment Brand relating to a claim or complaint concerning a Transaction.
“Security Standards” means all rules, regulations, standards, or guidelines adopted or required by the Payment Brands or the Payment Card Industry Security Standards Council relating to privacy, data security, and the safeguarding, disclosure, and handling of Payment Instrument Information, including, without limitation, the Payment Card Industry Data Security Standards (“PCI DSS”), Visa’s Cardholder Information Security Program (“CISP”), Discover’s Information Security & Compliance Program, American Express’s Data Security Operating Policy, MasterCard’s Site Data Protection Program (“SDP”), Visa’s Payment Application Best Practices (“PABP”), the Payment Card Industry’s Payment Application Data Security Standard (“PA DSS”), MasterCard’s POS Terminal Security program, and the Payment Card Industry PIN Transmission Security program (PCI PTS), in each case as they may be amended from time to time.
“Service Provider” means any party that processes, stores, receives, transmits, or has access to Payment Instrument Information on Merchant’s behalf, including, without limitation, its agents, business partners, contractors, and subcontractors.

“Settled Transaction” means a Transaction conducted between a Customer and Merchant utilizing a Payment Instrument in which consideration is exchanged between the Customer and Merchant for the purchase of a good or service or the Refund of such purchase and the value for such Transaction is settled by the Payment Brand through Processor to the Merchant.

“Transaction” means a transaction conducted between a Customer and Merchant utilizing a Payment Instrument in which consideration is exchanged between the Customer and Merchant.

“Transaction Data” means the written or electronic record of a Transaction, including, without limitation, an authorization code or settlement record, which is submitted to Processor.

“Transaction Receipt” means an electronic or paper record of a Transaction generated upon completion of a sale or Refund, a copy of which is presented to the Customer.