Merchant Account Request Form

Purpose:

- To request new merchant accounts for collecting debit/credit payment card revenue.
- To collect information needed to comply with the Payment Card Industry Data Security Standards (PCI DSS) and the UMB Procedure on Establishing and Accounting for Payment Card Accounts.

If a question does not apply, please mark as "N/A". If additional space is needed, please attach additional pages. Email the completed form and any attachments to DL-CITSPCICompliance@umaryland.edu.

Questions? Email DL-CITSPCICompliance@umaryland.edu.

Instructions

1. DEPARTMENT INFORMATION:

DEPARTMENT NAME: _____

DOING BUSINESS AS ("MERCHANT") NAME: _____

MERCHANT LOCATION ADDRESS: _____

MERCHANT DESCRIPTION: _____

2. PRIMARY CONTACT INFORMATION*:

CONTACT NAME:	_____	DEPARTMENT:	_____
CONTACT TITLE:	_____	EMAIL ADDRESS:	_____
MAIN TELEPHONE :	_____	ALT. TELEPHONE:	_____

LIST ALL EMPLOYEE AND AUTHORIZED AFFILIATE EMPLOYEE NAMES, TITLES, AND EMAIL ADDRESSES WHO WILL BE INVOLVED WITH PROCESSING PAYMENT CARD TRANSACTIONS (Attach a file if needed):

*The PCI Compliance Committee will reach out to the Primary Contact listed above to schedule an Onboarding meeting.

3. PCI COORDINATOR CONTACT INFORMATION:

If the PCI Coordinator is the same individual listed as the Primary Contact above, insert "Same as Primary Contact" in the PCI Coordinator Name field.

PCI COORDINATOR NAME: _____ DEPARTMENT: _____
PCI COORDINATOR TITLE: _____ EMAIL ADDRESS: _____
MAIN TELEPHONE : _____ ALT. TELEPHONE: _____

4. MERCHANT INFORMATION:

DEPARTMENT WILL ACCEPT PAYMENT CARDS (Check all that apply):

❑ In Person

❑ Events where mobile equipment is required to take payment

❑ By Phone

❑ By Mail

❑ On line Payment via University Provided Gateway/Application (TouchNet/MarketPlace)

❑ Online Payment via Department Selected Gateway/Application (provide details in Section 5)

GIVE A BRIEF DESCRIPTION OF YOUR PAYMENT CARD PROCESSING NEEDS (Describe how and in what capacity you will process, transmit and/or store cardholder data):

DEPARTMENT REVENUE OBJECT AND SOAPF

DEPARTMENT STAFF RESPONSIBLE FOR PROCESSING CHARGEBACKS / REFUNDS / VOIDS:
Please attach additional names and contact information if needed.

NAME: _____ TITLE: _____
EMAIL: _____ TELEPHONE: _____

DEPARTMENT SOAPF FOR MERCHANT BANK PROCESSING FEES (Expense Object 4945)

5. DEPARTMENT SELECTED GATEWAY/APPLICATION INFORMATION: (If you are not using a Third Party Processor or Gateway, please go to SECTION 6.)

1. Is a list of service providers (vendors) maintained including a description of the service(s) provided? Service providers are web application and payment gateway vendors contracted to collect information and process payment card payments.

   YES (__) NO (__) If NO, please explain _____

2. Please list all of the service providers below:

3. Do you have a written agreement with an acknowledgment that indicates that the service provider (vendor) is responsible for the security of cardholder data?
   YES (__) NO (__) If NO, please explain _____

4. Has the written agreement been reviewed and approved by Strategic Sourcing and Acquisition Services (SSAS)?
   YES (__) NO (__) If NO, please explain _____

5. Has the written agreement been reviewed and approved by the Center for Information Technology Services (CITS) department?
   YES (__) NO (__) If NO, please explain _____

6. Will you have a program in place to validate the service provider's (vendor's) PCI DSS compliance status before engaging in a new relationship?
   YES (__) NO (__) If NO, please explain _____

7. Will you validate the service provider's (vendor's) PCI DSS compliance status at least annually?
   YES (__) NO (__) If NO, please explain _____

8. Is there a website that is used to collect customer payments?
   YES (__) NO (__) If yes, what is the website?
   _____

6. REQUIRED PCI COMPLIANCE INFORMATION:

All Employees and Authorized Affiliate Employees who are involved with processing payment cards **must comply** with applicable policies and procedures, including:

- UMB Procedure on Establishing and Accounting for Payment Card Accounts
- UMB Policy VIII-99.08(A) on Payment Card Industry Data Security Standards

- Procedure on Payment Card Industry (PCI) Data Security Standards (DSS) Compliance and Payment Card Transactions
- UMB Procedure on Establishing and Accounting for Payment Card Accounts
- UMB Policy X – 99.11(A) Incident Response Policy
- UMB Policy X – 99.16(A) Protection of Confidential Information

All Employees and Authorized Affiliate Employees who are involved with processing payment cards **must successfully complete** the required PCI training in the Learning Management System (LMS). All Employees and Authorized Affiliate Employees can access the LMS via the UMB portal. The "PCI Simplified" training is located in the Library under the IT Security category.

The PCI Compliance Committee will reach out to the Primary Contact listed above to schedule an Onboarding meeting.

Merchant Account Request Form Instructions

The Merchant Account Request Form is required to establish a merchant account for collecting debit/credit card payment revenue from external sources. The form is administered jointly by the Office of the Controller – Student Financial Services (OOTC-SFS), the Center for Information Technology (CITS), and the PCI Compliance Committee. Refer to the Procedure on Establishing and Accounting for Payment Card Accounts for guidance.

Section 1: Department Information

1. Department Name: Enter the name of the department that is responsible for managing the sales transactions for the merchant account.
2. Doing Business As: Enter the name of the business (if applicable). Example: Dental Clinic.
   This name will appear on the bank statements.
3. Merchant Location Address: Enter the address where the debit/credit card equipment is located.
   Example: Penn Garage, 120 S. Penn St., Baltimore, MD 21201
   If transactions are only conducted via the Internet, enter the physical location of the sales office.
   Example: Cashier's Office, 601 W. Lombard Street, Suite 206, Baltimore, MD 21201
4. Merchant Description: Describe the goods and/or services provided.
   Example: Receive payments from students for tuition and fees.

Section 2: Primary Contact Information

The Primary Contact is the individual who oversees the financial transactions for the merchant account. Examples include an Administrator, Budget Director, Department Head, etc.

1. Enter the Primary Contact information.
2. Enter information for all individuals who will be involved in processing transactions.

Section 3: PCI Coordinator Information

Each Operational Unit must have a designated UMB employee who will have primary authority and responsibility for payment card transaction processing within that Operational Unit. The appropriate Dean or Vice President office will maintain the list of primary UMB Employees with this designation ("PCI Coordinator"). The PCI Coordinator cannot be an Authorized Affiliate Employee.

The PCI Coordinator is responsible for ensuring:

- Compliance with PCI DSS.
- Only appropriate individuals have access to payment card transactions or CHD.
- Individuals with duties related to payment card transactions, including refunds and chargebacks, successfully complete the mandatory annual training provided in the Learning Management System (LMS).

Information on PCI DSS compliance is available in the UMB Policy VIII-99.08(A) on Payment Card Industry Data Security Standards and the accompanying Procedure on Payment Card Industry (PCI) Data Security Standards (DSS) Compliance and Payment Card Transactions.

Section 4: Merchant Information

1. Check all of the applicable methods for accepting payments. Only authorized bank equipment supplied by the merchant bank can be used to process payment card transactions. The only merchant bank authorized by the State Treasurer's Office is BB&T/Truist. Please review the Procedure on Payment Card Industry (PCI) Data Security Standards (DSS) Compliance and Payment Card Transactions to determine requirements for handling payment cards under each method.
2. Describe how cardholder data will be processed, transmitted, and managed (i.e. stored, destroyed). Refer to the Procedure on Payment Card Industry (PCI) Data Security Standards (DSS) Compliance and Payment Card Transactions for guidance.
3. Provide the revenue Object and the SOAPF to be used for recording revenue.
4. List the individual who will be responsible for processing chargebacks, refunds, and voids.
5. Enter the SOAPF for recording the merchant bank fees. These fees will be charged to Object 4945 – Bank Fees.

Section 5: Department Selected Gateway/Application Information

TouchNet is the UMB provided gateway. Complete this section **only** if a service provider other than TouchNet will be used for processing payment card transactions.

If the department will use an alternate service provider and additional assistance is needed in completing this section, email DL-CITSPCICompliance@umaryland.edu

Section 6: Required PCI Compliance Information

PCI compliance and attestation are required by credit card companies. This section provides resources and information on PCI Compliance. Email questions to DL-CITSPCICompliance@umaryland.edu