# TN [Merchant Name] Payment Card Handling Procedures

**Purpose**

These card handling procedures document how credit card payments are handled for the merchant called [enter merchant name]. These procedures are in accordance with the standards established by the **Payment Card** Industry Security Standards Council (PCI SSC) and [W&M Payment Card Policy & Procedures](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/index.php). [Merchant name] is responsible for ensuring all processes, procedures, and technologies follow the security standards dictated by the PCI DSS and as approved by Financial Operations, Information Technology, and the PCI Committee.   In addition, if [name of merchant] has not had any transactions in the past 12 -18 months, [name of merchant] will be terminated.

**Business Process - Accepting and Handling Card Payments**

[insert summary of business process – description of the purpose of the TouchNet uStore/uPay site and type of business conducted.] Appendix A depicts the credit card data flow.

**User Access and Physical Security:**

Access to cardholder data TouchNet is authorized by the designated merchant manager. Access to TouchNet is managed by Information Technology. The merchant manager requests access for each departmental user through RequestIT ([support.wm.edu](https://support.wm.edu/CherwellPortal/IT2?_=29667f62)). The online request must uStore/uPay site, and role. (See Appendix B for TouchNet roles.) All logins to TouchNet are unique to the user and should NOT be shared with anyone.

A complete listing of who has access to this merchant can be found online in TouchNet for this merchant and serves as the Employee Log. Only the merchant manager, designated W&M Bank Reconciliation Accountants, [and any department users] have access to TouchNet [store name or upay site name]. The merchant manager reviews access annually as well as when personnel leave the department. All terminations are reported to IT for modifications in TouchNet access and to the PCI Committee (pci@wm.edu).

**Annual Training:**

In accordance with PCI DSS Requirement 12.6.1, all users within the department authorized to handle card payments will complete the annual W&M Payment Card Industry DSS training as follows:

* W&M Payment Card Industry Training
* W&M Security Education and Awareness Training
* Merchant Manager Training
* Payment Card Security and Confidentiality Agreement
* Payment Card Merchant Manager Agreement
* Reviewing the Department Card Handling procedures
* All associated policies and procedures as referenced on the W&M website for [Payment Card Handling](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/index.php)

Employees will access this training through Cornerstone; students and volunteers will access it through Blackboard. This annual PCI DSS training is intended to promote employee awareness of technical and operational requirements to protect cardholder data. Upon hire, the department’s Merchant Manager directs the new employee to Cornerstone to complete the training. If the new employee is a student or volunteer, notify the PCI Committee (pci@wm.edu) so access can be granted to the Blackboard class.

Departments are responsible for tracking the initial training(s) and annual recertification(s), annual Payment Card Security and Confidentiality Agreement(s) and user access status using the [**PCI DSS Security Awareness Program Roster**](https://www.wm.edu/offices/financialoperations/paymentcardprocessing/paymentcardforms/pci-awareness-roster.xlsx).

**Payment Card Terminals:**

[Merchant Name] does not use a payment card terminal.

**Online Card Services**:

[Merchant Name] uses the integrated [uStore name/uPay site name]. TouchNet is an approved W&M ecommerce solution.

* [Merchant Name] only handles payment card transactions that have been processed through the TouchNet uStore/uPay. Neither [Merchant Name] nor authorized departmental personnel process face-to-face transactions where card information is entered directly into a website for a customer as this is not compliant with PCI DSS and violates W&M compliance.
* Each authorized user has a unique login/password. The merchant manager requests users to be setup in TouchNet via IT. Each user creates their own password.
* [Merchant Name] does NOT direct a payer to a specific computer or offer to enter payment card data into a website on their behalf. Admissions personnel will advise the individual to use “any internet enabled device” to complete the transaction on their own.

**Batch Settlement:**

Not applicable

**Banner Cashiering:**

[Merchant Name] TouchNet uStore/uPay site has a General Ledger integration to Banner. [Confirm this is true for your merchant.] Funds are posted to Bannerbased on the merchant account ID and index provided to Financial Operations on the W&M Payment Card Application. The W&M Bank Reconciliation Accountant reconciles monies received at the bank with TouchNet and Banner each business day. The Merchant Manager is contacted with any issues of reconciliation or General Ledger Exceptions.

**Disputes and Chargeback:**

Disputes and chargebacks are typically reported to the Cashiers Office. If [Merchant Name] merchant receives any dispute or chargeback directly, the Cashier’s Office is notified immediately upon receipt. The chargeback can either be accepted or rejected. If rejected, the merchant will provide supporting documentation to justify that the transaction is valid. Failure to respond within the allocated timeframe will result in a loss.

**Equipment & Use Overview:**

|  |
| --- |
| [Merchant Name] does not use external equipment. |
|  |

**Physical Security Procedures**:

Not applicable

**Payment Card Processing Procedures –**

1. **Online Orders**
	1. Online payments are received via the [ustore name or upay site name].
	2. [Merchant Name] does **NOT** submit orders on behalf of the customer.
	3. Only authorized users have access to TouchNet.
	4. Departmental personnel have a limited view of cardholder data in TouchNet.
2. **Mail Order – No credit card orders are accepted by mail.**
3. **Fax Order – No credit card orders are accepted by FAX.**
4. **Phone Order – No credit card orders are accepted over the phone.**
5. **Email Order – W&M does not accept credit card numbers sent in via email.**
	1. The credit card payment will NOT be processed. If numbers are received via email a response will be sent to the customer.
	2. The response will be a separate email – not a response to the original email, indicating the policy and procedure for sending credit card information.
	3. The email will be permanently deleted from email in box and trash.
6. **In Person – No credit card orders are accepted in person.**

**Refund Procedures:**

The TouchNet uStore/uPay site has a posted refund policy within the store. Each customer must acknowledge the policy before the sale is finalized in TouchNet.

Procedures to refund a credit card transaction are included in the user manual for TouchNet.

**Incident Response Procedures:**

An incident is defined as a suspected or confirmed data compromise in which there is a potential to impact the confidentiality or integrity of payment card data.  A data compromise is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted payment card data is collected, processed, stored, or transmitted.

In the event of a suspected or confirmed incident the merchant manager personnel will:

1. Call theChief Information Security Officer at 221-1822 or email abuse@wm.edu with a description of the incident.
2. Do NOT turn off the PC.
3. Disconnect the network cable connecting the PC to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
4. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
5. Assist the Response Team as they investigate the incident. Revisions/Approvals

| Ver. # | Changes By | Ver. date | Reason |
| --- | --- | --- | --- |
| 1.0 | Bonnie Fleming | 8/1/2021 | Departmental Procedures – TouchNet template Drafted |
| 3.0 | Bonnie Fleming  | 8/15/2022 | Revisions |
| 3.0 | Kelly Johnson | 9/26/2022 | Clause added under Purpose regarding merchant termination. Access Log retired; PCI DSS Awareness Log added in its place at every mention.  |

## Appendix A – Data Flow

##

## Appendix B – TouchNet Roles

## uPay Roles

|  |  |
| --- | --- |
| Site Manager | * Manage the allowed payment methods
* Configure the site to accept recurring payments
* Configure site links and URLs
* Configure e-mail announcement text
* Configure layout templates
* Configure additional donation offerings
* Take uPay sites online or offline
* Search for payments
* Cancel/refund payments
* Review Marketplace financial reports for the uPay site
* Refund a single payment, or a group of payments
 |
| Payment Clerk | * Search for Payments
* Cancel/Refund payments
 |
| Accountant | * View Marketplace financial reports for the uPay site
 |

## uStore Roles

|  |  |
| --- | --- |
| Store Managers | * Manage general store settings
* Bring stores online and take stores offline (and schedule status changes)
* Configure text messages
* Configure stores to run in single-store mode
* Upload splash and side banner images, and for stores in single-store mode, upload header images
* Upload additional images for use with style sheets
* Download, upload, and activate style sheets for stores in single-store mode
* Configure shipping classes and rates
* Configure store product categories
* Add and edit products
* Configure an additional donation to be offered during checkout
* Schedule status changes for products
* Move products between categories
* Configure payment methods that are allowed with user groups
* Configure user modifiers
* Activate the Marketplace tax service and configure which states can use this service
* Grant the store clerk, fulfiller with refund/cancel rights, and fulfiller user roles to other users
* View Marketplace financial reports for the store
 |
| Store Clerks | * Add and edit products in their assigned store and move products among categories
 |
| Fulfillers with refund/cancel rights | * Fulfill orders
* Refund orders
* Cancel orders
* For orders made with an ACH payment method, override the waiting period and proceed with ful-fillment
 |
| Fulfillers | * Fulfill orders
 |
| Store Accountants | * View Marketplace financial reports for the store
 |

## Administrative User Roles

|  |  |
| --- | --- |
| Chief Administrator | * Manage administrative site settings
* Upload header and splash page images
* Create and maintain store categories
* Create and maintain product categories
* Name delivery methods
* Create accounting codes and assign an accounting code for taxes
* Modify the store listing order
* Enable text message alerts
* Configure the storage allocation for each store for digital products and specify the maximum file size
* Delete unused payment methods saved by uStores registered users
* Update store cache settings
* Download, upload, and activate style sheets
* Grant the chief administrator, administrator, accountant, and merchant manager roles to other users
* Add uStores user groups
* Manage uStore user authentication settings
* Add new merchants
* Review Marketplace financial reports
 |
| Administrator | * An administrator can do everything a chief administrator can, except add other chief administrator or other administrators
 |
| Accountant | * Review the Revenue by Merchant report
 |
| Merchant manager | * Manage general merchant settings
* Grant the store manager and uPay site manager user roles to other users
* Add stores or uPay sites for the assigned merchant
* Edit general settings for stores created under the assigned merchant
* Add accounting codes and assign the accounting code used for taxes
* Review Marketplace financial reports
 |