Procedures to Open a Credit Card Merchant Account

All credit card merchant sites must be established and maintained through Cash Management, Accounting Services. All Revenue must be deposited into a UW Madison bank account which posts to Wisdm.

Review the following information prior to submitting a new Credit Card Merchant ID Request:

- Merchant accounts may be set up for either e-commerce online payments or for electronic payments which are made directly at the point of sale. E-commerce payments are payments that are accepted online via a website which connect to a PCI DSS compliant application. Electronic payments are used when the credit card is present, for mail orders, phone orders, or faxed orders which use a dedicated PCI Compliant terminal.

- Revenue from merchant account sales will be deposited into the UW Madison’s bank account. The revenue will post to WISDM two days after the transaction to the funding provided on the Credit Card Merchant ID Request Form.

- Expenses associated with credit card sales are billed directly to the Merchant ID on a monthly basis. The expenses that post to WISDM contain the previous month’s fees. Expenses may include credit card terminal cost for electronic merchant accounts, and transaction fees.

- Elavon processing fees are approximately 2% of each transaction, $5.00 for the monthly maintenance fee, and $7.50 for chargeback fees. American Express charges 2.1% of each transaction.

- The standard set up for a new merchant account includes MasterCard, Visa, and Discover. Should the department decide to choose to accept American Express cards, an additional reconciliation and an additional connection is required.

- To request a new credit card merchant account, complete and submit the Credit Card Merchant ID Request Form [https://charge.wisc.edu/info/account_request.asp](https://charge.wisc.edu/info/account_request.asp). The Divisional Business Representative (DBR) must approve the new merchant account and if the merchant account is e-commerce or electronic. The DBR should also determine which card brands the new merchant will accept.

- The Merchant is required to contact Cash Management [pci-help@bussvc.wisc.edu](mailto:pci-help@bussvc.wisc.edu) to obtain access to Merchant Connect (MCP). Merchant Connect is an online tool from Elavon, the credit card processor, which displays transaction activity and monthly statements. The Merchant must reconcile transactions to WISDM daily, weekly, or monthly depending on volume.

- The PCI Site Manager must schedule a PCI Site visit with the PCI Compliance Team at [pci-help@bussvc.wisc.edu](mailto:pci-help@bussvc.wisc.edu) to activate their new merchant account. The PCI personnel will come to the merchant’s site to review the new merchant business procedures and assist with the SAQ.

- The PCI Site Manager must submit the business procedures and continuity plan for taking credit card payments to CASH Management to [pci-help@busscs.wisc.edu](mailto:pci-help@busscs.wisc.edu) prior to activating the merchant account.
Electronic Payments for Face-to-Face/Counter, Mail order/Telephone, or Point of Sale (POS) with use of an EMV Chip or Swipe machine

Contact Cash Management for equipment types and pricing information. Standalone credit card machines will ship directly from Elavon to the department. The cost of the new credit card machine will be charged to the merchant ID.

- When the equipment arrives, verify the machine has the correct address, merchant name, and Merchant ID on the machine when it is turned on.
- The credit card machines are programmed for dial out and require a regular analog dedicated phone line. There are different PCI Requirements if Ethernet is used. For further information please contact PCI-Help@bussvc.wisc.edu.
- Call Elavon training at 866-451-4007 to schedule a 20 minute training on how to use the credit card device and transaction settlement. Terminal will not auto settle unless the machine is turned on.
- Record the serial number and manufacturing information at https://charge.wisc.edu/users.
- The merchant must make a new sticker to place on the terminal containing this information:
  - Equipment problems Relationship Premier Services 800-725-1245 Option 2
  - Supplies such as thermal paper call Customer Service Center at 800-725-1243 Option 3
  - Elavon Training 866-451-4007

For POS systems contact PCI-Help@bussvc.wisc.edu.

Internet Storefront with CASHNet checkout

All merchants must use CASHNet for ecommerce or obtain approval from PCI CT to use another Service Provider. CASHNet is the ecommerce Service Provider contracted by the University of Wisconsin for credit card checkouts which will be connected to the newly assigned Merchant ID.

If your department already has a Merchant ID that uses CASHNet for check out, please talk with your DBR to see if the existing Merchant ID can be used by adding an additional location to it.

DoIT provides a centralized service that can be utilized for creating storefronts. Please contact Cash Management for more details at PCI-Help@bussvc.wisc.edu.

CASHNet instructions http://www.bussvc.wisc.edu/acct/policy/rpa/tabstorefront.html

- Provide a list of CASHNet operators with names and email addresses to Cash Management to obtain login information. CASHNet operators will be able to find transactions, obtain reports to aid in reconciliation, and process refunds in the application. Each person that will log into CASHNet must have a unique operator ID.
- There are no CASHNet settlements to Elavon on Saturday or Sunday, those transactions will be combined with Monday’s transactions. There will be 3 days in Monday’s settlement- Sat, Sun,
and Mon. Tues- Fri will contain one day of transactions only. CASHNet’s end of day settles at 9:00 pm.

- Send a JPEG file to Cash Management if a Logo is needed to be displayed on the customer payment page.
- The CASHNet account may only be turned on by Cash Management or official DoIT staff. Once the CASHNet store has been put into production, the storefront URL may be put up for customer’s access.

**Electronic, Paper Processing or Chargebacks**

There must be adequate physical security for all paper documents containing credit card information received potentially via telephone, fax, mail, or in person orders as well as chargeback documentation. This includes:

- The portion of the document containing the credit card number should be destroyed upon completion of the transaction. The remaining document should be maintained per UW System Administration policies. These guidelines can be found at [http://www.library.wisc.edu/archives/wp-content/uploads/sites/23/2015/08/Fiscal_Accounting_UWS2012.pdf](http://www.library.wisc.edu/archives/wp-content/uploads/sites/23/2015/08/Fiscal_Accounting_UWS2012.pdf).
- Fax machines must use an analog connection and must be located in a secure office that is locked when not in use. The fax machine should not have internal memory for storing received documents.
- Under no circumstances should the Card Identification Number (CID) be stored electronically or on paper. The CID number is the three-digit security code on the back of the credit card (MC, VI, Disc). The American Express CID number is a 4 digit number on the front of the card.
- Mail order forms with credit card information must be secured after the mail is opened. The department should ensure mail order forms are stored in a secure location.
- Credit card receipts may only show the last four digits of the credit card number.
- Chargeback documents from Elavon containing cardholder data must be secured until processed and destroyed (cross cut shredded) after processing. Chargebacks occur when the customer challenges the validity of the original charge and instructs their bank to reverse the charge.