# MERCHANT NEWS

**Be a part of the solution!**

VOL. 1, ISSUE 1 8.1.2014

## Top Stories


**Higher One CASHNet**

**Merchant Responsibilities**

**Reconciliation Procedures**


**Fact or Fiction ?**

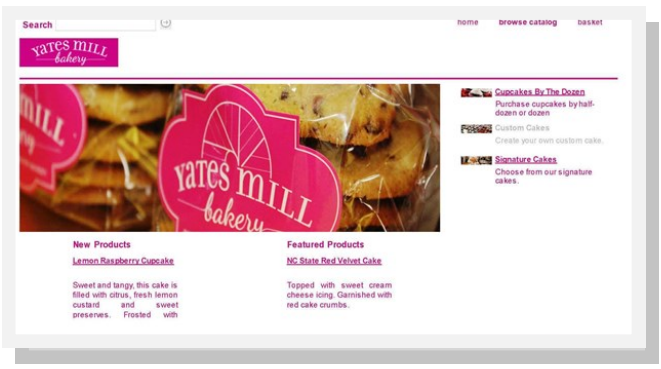
## HigherOne- CASHNet


Due to the growing and increasingly complex PCI compliance requirements, the University is streamlining its business process and reducing the number of ecommerce providers used. Over the next few months, Merchant Services, OIT, and EAS will be working with ecommerce merchants to move their current storefronts to HigherOne, the new ecommerce solution. All merchants accepting credit card payments over the internet will be required to use HigherOne-CASHNet by January 2015.

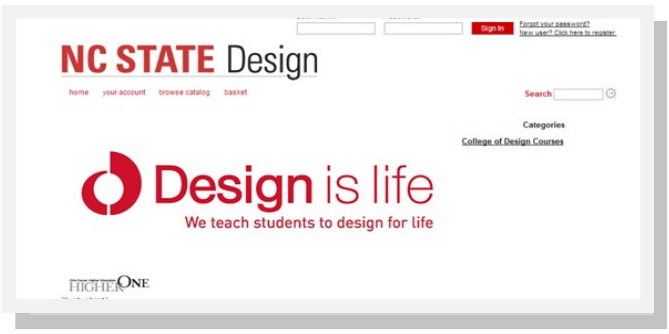
A University department may request an exemption from this requirement by providing a business case justifying an alternate vendor or process to Merchant Services. The business case will be reviewed and forwarded, as appropriate, to the PCI Team to request approval.

**Take a look at the website template options!**

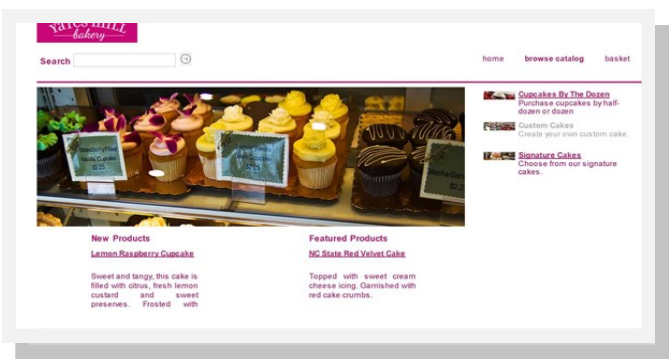
Default Theme




Layout 2 Theme




Classic Theme



## Merchant Responsibilities

NCSU merchants that accept credit cards have a responsibility to prevent and detect fraud. In order to do this, merchants need to follow the Payment Card Industry Data Security Standard (PCI-DSS)

At a minimum, merchants must complete the following items to be PCI compliant:

- Understand PCI-DSS requirements for your merchant type
- Prepare a list of business & technical/IT contact information as it relates to merchant business
- Prepare & maintain a data flow diagram (DFD)
- Prepare inventory of software & hardware used with merchant business ( Ex: POS terminal model or POS software version)
- If applicable, secure & maintain credit card terminals used to process sales
- Prepare a list of service providers used for merchant business (Ex: HigherOne)
- If applicable, ensure your third party provider(s) application and systems are PCI compliant
- Complete and sign merchant agreement annually
- Complete and sign self assessment questionnaire (SAQ) annually
- Attend PCI DSS training annually

**Notify Merchant Services immediately when changes occur with your merchant's business (change in DFD, service provider, personnel, business process, documentation, equipment).**

---

## Reconciling for POS Terminals & Third Party Applications

All University merchants are required to reconcile their merchant account. Merchants using a third party payment application must adhere to the following procedures:

1. Point of Sale terminals must be manually batched daily.
2. Purchases in Nelnet, HigherOne-CASHNet, Paypal, Yahoo, or Authorize.net (third party applications) are batched daily.
3. Print total sales report or batch reports, at least weekly, from third party application.
4. Compare the third party processor's report to WRS.
5. The third party application's report should match WRS.
6. If not, review transactions to find the discrepancy, and correct any errors.
7. Review monthly reports and supporting documents to ensure that all transactions are valid.

Remember, Merchant Services posts funds to your merchant account but does not verify that all funds have been received from your third party processor.

## Segregation of Duties

It is against University policy to have one person complete all accounting duties without review.

**One person cannot hold all of these positions.**

- User access to storefront
- User processing orders
- User processing refunds
- Reconciles third party application reports with WRS

**Merchants may combine the following roles:**

- Storefront access
- Processing Orders/Refunds

Reconciling role must be separate from processing role. Ideally access to storefront is separate from processor and reconciliation.

---

## Fact or Fiction?


**Rumor has it….**

**1. The University and Third Party Vendors must comply with PCI-DSS.**

Fact!

**2. All merchants will be PCI-DSS compliant by July 2015.**

Fact– The project team is working on various tasks to achieve our compliance goal.

**3. All merchants will use the eStore.**

Fiction– Merchants that need a more complex payment solution may apply for an exception.

**4. The University is limiting the number of service providers used by merchants.**

Fact– To meet compliance requirements, we must reduce service providers to a manageable level.

**5. Resources were allocated for PCI-DSS security.**

Fact– Budgeted resources were approved for FY 2015.

---

## Contact Information

For the most accurate and up-to-date PCI– DSS and merchant information, contact Merchant Services.

Merchant Services - merchantservices@ncsu.edu

Amanda Richardson – Manager
aarichar@ncsu.edu
(919) 513-4464

Taylor Chappell – Merchant Analyst
tbchappe@ncsu.edu
(919) 515-7004

Amanda Redic - Merchant Coordinator
alredic@ncsu.edu
(919) 515-7204