Payment Cards Processing at UNL

VOLUME 8, ISSUE 2 MAY, 2014

University of Nebraska —Lincoln
Bursar's Office

TSYS Conversion Continues to Create Problems for Merchants

We are continuing to work on the issues encountered since the conversion TSYS carried out February 1st. Some of the issues seen:

- Charges for incorrect equipment
- Charges for sales tax on equipment
- Chargeback activity appearing on statements with incorrect sign resulting in an overstatement of sales activity
- Chargeback activity not appearing on statements at all
- Adjustments not correctly displayed on statements resulting in incorrect figures for sales activity
- University funds settlement issues
- Delays in receipt of merchant statements and manner in which they are received

Please be sure to review your merchant statements closely and contact us with any issues seen.

As you can see, this has been quite a challenge. We have made some corrections already and been in contact with those departments. Things are improving, but we are not cleared of all the issues. It is a continual challenge to try to track the issues still pending and new ones as they occur each month. Thank you all for your understanding and patience as we work through the problems.

Fiscal Year End Approaching

Fiscal Year End is quickly approaching. Please submit your monthly sales report as soon as possible after June 30th. That will assist us in completing the sales and fee allocation as early as possible in July. The sales and fees will both be posted in FY 2014.

Deferred revenue for those figures in our "Amount Not Yet Posted by Bank" column of the June sales worksheet are posted by the Accounting department. So please contact them prior to booking any deferred revenue.

Target Breach Yet Another Reminder of PCI Importance

It's hard to contemplate the number of people affected by the recent Target breach. An estimated 110 million customers had payment information stolen resulting in an enormous amount of frustration, insecurity, and a huge reissuance of cards. The following was taken from the Shopatron blog article "How to Avoid Being a Target: 6 Lessons Learned from Target's Data Breach" published February 27, 2014.

Here are six ways to defend your business:

1) Have someone who understands security—and use them as a resource. Involve them in decision-making processes. Talk to your specialist about new technology you're considering and how to implement it securely. The security professional is not there to cause stress or paranoia, but simply to make sure you have all the necessary information to make good choices.
2) Understand that *everyone* is part of the security team.
3) Treat your vendors like part of the team, too. Everyone who becomes a vendor can assist with security —or make you less secure.
4) Do a risk assessment. Security isn't about eliminating risk (that's nearly impossible), but understanding it.
5) Know what's on your network. Sit down with an IT person and ask them.
6) Keep your software up-to-date.

Consider this: The likelihood that someone outside your company knows more about hacking a system than you know about defending it is extremely high. Be aware of the risks.

University of Nebraska —Lincoln
Bursar's Office

121 Canfield Administration Bldg
Lincoln, NE 68588-0412

Phone: 402-472-1734
Fax: 402-472-2959
E-mail: bursar@unl.edu

The Office of the Bursar is responsible for administering the University of Nebraska-Lincoln money handling policies and procedures. Don't ever hesitate to contact us with any receipting questions you may have.

PCI DSS / Self-Assessment Questionnaire Version 3.0

Next fiscal year's compliance, July 2014 - June 2015, will apply Version 3.0 of the PCI DSS and it's counterpart Self-Assessment Questionnaires (SAQs).

With PCI DSS Version 3, there are new SAQs as well as updated eligibility criteria for existing SAQs. Departments will need to evaluate the eligibility criteria to understand which SAQ will be right for them. The two new SAQ's are SAQ A-EP and SAQ B-IP.

Each of the SAQ's has also been updated to provide more guidance and clarification of expectations. You will see that the format is altered as well as the content in some cases.

Key themes of the new version are outlined below as taken from the PCIDSS Council website "PCI-DSS and PA-DSS – Version 3.0 Change Highlights" document:

Key Themes

Changes planned for Version 3.0 are designed to help organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice. Key themes emphasized throughout Version 3.0 include:

Education and awareness

Lack of education and awareness around payment security, coupled with poor implementation and maintenance of the PCI Standards, gives rise to many of the security breaches happening today. Updates to the standards are geared towards helping organizations better understand the intent of requirements and how to properly implement and maintain controls across their business. Changes to PCIDSS and PA-DSS will help drive education and build awareness internally and with business partners and customers.

Increased flexibility

Changes in PCIDSS and PA-DSS 3.0 focus on some of the most frequently seen risks that lead to incidents of cardholder data compromise - such as weak passwords and authentication methods, malware, and poor self-detection thereby providing added flexibility on ways to meet the requirements. This will enable organizations to take a more customized approach to addressing and mitigating common risks and problem areas. At the same time, more rigorous testing procedures for validating proper implementation of requirements will help organizations drive and maintain controls across their business.

Security as a shared responsibility

Securing cardholder data is a shared responsibility. Today's payment environment has become ever more complex, creating multiple points of access to cardholder data. Changes introduced with PCIDSS and PA-DSS focus on helping organizations understand their entities' PCIDSS responsibilities when working with different business partners to ensure cardholder data security.

Since the new version has now been introduced, you can look for notices from us as we will be holding merchant meetings to discuss the impact of the PCI requirement changes on all UNL merchants and how to comply with them in a "business as usual" approach (meaning how to maintain our compliance efforts on a day to day basis).