Memo

To: UofL Credit Card Merchants

From: Jill Riede, Merchant Services Manager

CC: David Woods, Asst. Treasurer

Larry Zink, Controller/Treasurer

Date: October 18, 2011

Re: PCI DSS Compliance

By now you should be aware of Payment Card Industry Data Security Standard (PCI DSS) and how important it is to the University to protect cardholder data and to avoid a possible credit card breach. Anyone who collects/receives, stores, processes, or transmits cardholder data falls under the PCI guidelines. As part of our continual PCI DSS compliance efforts, UofL hired Walt Conway, Qualified Security Assessor (QSA), with 403 Labs, to conduct our PCI Gap Analysis. Hiring a QSA helps to ensure the University is taking all the necessary precautions and implementing processes to achieve and stay 100% PCI Compliant. PCI Compliance is a never ending task and will take all of us working together to achieve and maintain successful compliancy.

Walt visited UofL August 30, August 31, September 1, and together with the PCI Committee *(David Woods, Andrew Davis, Matt Witten, myself)* we were able to meet with the larger and/or more complex merchants: Athletics, Advancements, Parking, Dental School, Bursar, Housing, Delphi, and IT. We wanted to share what we learned from this analysis. My goal is to reach out with the rest of the credit card merchants by year end to conduct a mini-PCI Gap Analysis. Andrew Davis, IT, will be concentrating on implementing the Intrusion Detection System (IDS) and finish up moving the Virtual Terminals into PCI vlan's by year end.

PCI Compliance in Higher Education is complicated. One reason is a University is not a typical 'merchant'. Instead, a University is more like a city with many individual merchants accepting credit cards over multiple channels and using a variety of third party and/or service providers. UofL's decision on how to handle our third parties and service providers directly impacts the cost of PCI Compliance. We will be following up at a later date on this particular issue.

3 Digit Security Code:

The three (3) digit security code located on the signature panel on back of the credit card **IS NOT REQUIRED** for PCI purposes nor for better processing rates. This code can still be requested and keyed**,** however, we can **NO LONGER** record or store this information on paper due to higher and more costly mandates to be put in place. This includes any documents you have stored on paper, scanned, and archived. The three (3) digit code *(blacked out, taped out does not count)* needs to be physically cut out and discarded. If the three (3) digit code is cut out by itself you can simply throw away as the code is useless without the credit card number. If your department decides that none of the credit card data information is needed once the transaction has been processed then cross-cut shred the information immediately.

We recommend your department remove this question/prompt from the stand-alone credit card terminals and virtual terminals (*dedicated workstations/desktops/laptops*). If you have a stand-alone terminal such as a Tranz 330, Vx510, Vx610 you will need to contact Elavon, the University's credit card processor, 1-800-725-1245, Option 1, to have this completed.

For those using a Virtual Terminal *(dedicated workstation/desktop/laptop,)* I will be removing this question/prompt in the next few weeks. No action is needed on your part.

This field DOES NOT need to be deleted as a question from a website since UofL does not store this information – the credit card processor stores.

Credit Card Form:

If your department uses a form(s) for telephone, mail-in, or walk-in credit card transactions, we recommend you re-design that form to place cardholder data on the bottom portion. This design will make it easier to cut off and shred any cardholder data while able to save the top portion. Feel free to reference the Bursar credit card authorization form. As a reminder, if you continue to save paper containing the card number after you process the card transaction, those forms need to be kept in a locked cabinet with a paper access log recording each time a form is added or removed from the secure storage.

If you scan or copy the form and you do not physically remove the cardholder data before scanning or copying, then you need to mask all but the last four (4) digits of the card number with tape or otherwise obscure them *(e.g., with a black marker)* before scanning. The original form should be securely shredded after scanning *(or copying)* since it contains the card number.

NOTE: Should you use the University's OnBase and/or Knowledgelake/SharePoint scanning systems, you can use the image editor feature if installed. Therefore, once the document is scanned and saved as a TIIF you can use image editor to mark through the sensitive data and be sure to save in the same TIIF format. This is compliant since the marked thru data CANNOT be un-masked.

Email Credit Card Transactions:

Credit card data should never be accepted and processed if received via email. If you do receive an email, delete the email immediately and do not process the transaction. Alert the sender accordingly and provide alternative means of payment (mail, phone, web). On a side note, procurement card numbers or gift card numbers should not be saved on workstations and never send the number outbound in an email.

Fax Credit Card Transactions:

Any fax machine used to receive payment transactions must be located in a secure area, not available to the public or unauthorized staff members. Incoming faxes with payment card data should be removed as they are received and either processed immediately or stored securely until the transaction can be processed. Unless the machine is in a locked office without after-hours access *(including maintenance and cleaning personnel),* it should be active only during business hours. That is, fax machines receiving card transactions should be turned off at the close of business and on weekends and holidays, if not in a locked office without employee access.

Third Party or Service Providers:

UofL is involved in credit card processing for at least one third-party merchant on campus since Sodexo handles dining facilities. Processing transactions or providing services that can affect the security of those transactions *(e.g., managing firewalls, hosting application servers)* for any unrelated third party risks the University having to validate its PCI compliance as a service provider and not as a merchant. The validation process for service providers is much more rigorous and expensive. As mentioned earlier, this will be addresses at a later time with the applicable departments.

Training:

Colleges/Schools/Departments that process their credit card transactions with Elavon, our credit card contracted processor, received an online training email late September/early October requesting completion by October 31, 2011. Training will be required annually.

Corporate & Departmental Security Policy:

Each department that accepts credit cards for payment is responsible for maintaining complete and accurate records regarding its credit card transactions and safeguarding cardholder data in accordance with PCI standards. This includes having a policy which would include training a new employee on the credit card process. The University-wide Incident Response Plan (IRP) with PCI additions will be finalized and posted on the Treasury Management website by year end. This IRP will include the departments' responsibility should you suspect unusual credit card activity.

The corporate PCI DSS policy as well as other PCI related documents are available on the Controller's website:

Conclusions:

The University is not PCI compliant today. We do however, have a clear path forward that can allow us to reduce our PCI scope significantly and simplify its validation process. Achieving PCI compliance will require a significant commitment of business and IT resources, particularly during the PCI remediation and compliance validation stages. Our PCI Team is committed, informed, and will continue to work together effectively.

We expect a significant commitment of staff, resources, and budget over the course of this initial compliance effort and continuing in subsequent years.

FOLLOW UP NEEDED:

Please send me an email by Friday, November 11, 2011 with your current process and what changes will be made to implement the aforementioned items and completion date.

Feel to free to call 852-0892, email me directly or email the Treasury Management Service Account with any questions.

Thank You