Payment Cards Processing at UNL

VOLUME 9, ISSUE 2

FEBRUARY, 2015

University of Nebraska —Lincoln
Bursar’s Office

Some Items Taken from Continuum Sessions

I hope you were all able to take advantage and attend the Continuum sessions offered at the beginning of the month. They were very informative and having the numbers we had in attendance really assisted in covering a lot of topics in those three days. A big thanks to all who participated!

For those not present, you have some catching up to do. It will be even more important that you closely follow ALL INFORMATION we send to the UNL payment card community through these newsletters and other communications. Be sure to read all correspondence and follow through on any action required for your merchant accounts. Ultimately, each department knows their processes best and is responsible for ensuring adequate and proper security of their payment card transactions.

Here are just a few of the topics discussed in the training sessions:

**Video Surveillance**

Do you have video surveillance in an area where cards are processed? If the video records card numbers or you can determine the card number entered by the video coverage, the video is then in scope.

**ACTION:** Determine if you have video surveillance in areas where payment card numbers are entered or swiped into terminals or computers. If it exists, ensure no card numbers are in any way captured by your video surveillance. Alter the angle or position of your cameras to ensure they are NOT capturing this data. If this is problematic, other alternatives may also be available to accomplish this.

**Voice Mail**

Do you accept credit card orders by phone? Does that phone line have voicemail? Credit card numbers should not be left on a voicemail. If that is your business practice, the entire voicemail system becomes within PCI scope. Even worse, if your voicemail goes to email, the entire email system is in scope.

**ACTION:** Be sure your business practice is to NOT accept card numbers via voicemail. If you have voicemail on a phone line used for taking orders, have your message say something like this: “Do not leave your card number in your message. Please call back during our normal business hours and give it to a customer service representative.” If a customer still chooses to leave it in a message, that would be considered ‘incidental’ and does not bring these systems into scope.

**Card Numbers on Paper**

Do you have card numbers written on paper? These must be kept secure from the time they are received until the point they are destroyed. Destruction must be by one of these methods: 1) cross-cut shredded, 2) incinerated, or 3) pulped. After processing of the payment, it is good practice to either remove the card number from the paper form and destroy it at that time or at least black out the card number (or all but the last four digits) until it can be properly destroyed. All documentation containing payment card numbers must be destroyed after its useful life has expired, or 13 months. See Requirement 9.7-9.8 of the PCI DSS v3.0 for further details.

**ACTION:** Review your processes to determine where you have card numbers written down and be sure your processes are in compliance.
UNL Processing Standards Tightened as Result of v3.0

UNL has a sizeable credit card community that is continually changing to meet the perceived needs of our customers. In order to comply with the more rigorous PCI requirements of 3.0, we must look at standardizing our processes in order to make this community manageable. Standardizing means we may have to eliminate some processing options that are currently used. As we go through the scoping engagement with our Qualified Security Assessor (QSA), areas of opportunity to reduce our scope will be identified. We will then determine what our standards will be based upon an overall assessment of the University business processing needs. Based on our discussions thus far, the following standards will be implemented immediately:

Faxing Cardholder Data No Longer Allowed
Due to the expanding complexities of the inner workings of fax machines (i.e. VoIP and all-in-one fax units), our policy going forward will be to no longer allow acceptance of payment information via fax. We realize this may be a challenge for some departments. If you are have difficulty finding alternatives, please contact the Bursar’s Office with the details of your challenges, and we will work with you to find another acceptable process.

Emailing Cardholder Data Not Allowed in Any Way
The emailing of cardholder data is not allowed in current policies; however, some departments still accepted payment via this method (by creative means). This can no longer be done—even if the cardholder number is split into multiple emails. This practice was specifically asked of our QSA and is not in compliance. No cardholder data can be accepted in any way via email going forward. Again, please explore other ways of obtaining the cardholder data. If an acceptable alternative is not found, contact the Bursar’s Office with the details of your challenges, and we will work with you to find another acceptable method.

All Payment Card Processing Equipment and Software must be Purchased via the Bursar’s Office
It has always been strongly encouraged to purchase any card processing terminals through the Bursar’s Office. Moving forward this will be a requirement in order to ensure the equipment meets PCI regulations. As stated in the PCI training, our current terminals are no longer in compliance because they utilize SSL for transmission of the cardholder data, but the purchase of replacements is not immediately necessary. In fact, we discourage it. We will need to in the near future, but until we can confirm who our Acquirer will be going forward and are able to work with them on this compliance issue and the impending EMV requirements, any purchase may result in equipment that will ultimately not be needed or useful.