Payment Cards Processing at UNL

VOLUME 6, ISSUE 2 MAY, 2012

University of Nebraska —Lincoln
Bursar's Office

Credit Card Numbers -Do you *ever* have them in writing?

Do you:

- Take credit card numbers by mail or fax?
- Write down credit card numbers as orders are taken over the phone or in person?

Then this applies to you.

Per the PCI DSS requirements, we must:

Restrict access to cardholder data by business need to know.

and

Restrict physical access to cardholder data.

Care must be taken at all times for any paperwork with credit card numbers on it. This means that the information must be secured, from the time we receive a payment form or record a credit card number on a form, until it is properly destroyed. (See PCI DSS Question 9.6)

Credit Card Number Cycle
Receive/Record > Process > Store > Destroy

Do you black out the card numbers on your forms? That is a great way to protect the card number, but it is not sufficient to pass requirements for destruction of the data. Files—even with the card numbers blacked out–must be maintained securely until they are destroyed by cross-cut shredding.

How do you purge your documents? All paperwork with card numbers must be cross-cut shredded when destroyed. If not, there is still a chance that the numbers could be accessible. Take a close look at the picture below. This shows the results of a strip-cut shredder. Although the likelihood of this every being discovered and used by a criminal is very low in our opinion, it demonstrates why the PCI DSS requires a cross-cut shredder to destroy documents with credit card numbers. (See PCI DSS Question 9.10)

See Requirements 7 and 9 of the SAQ for further information regarding these requirements.

https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs

Monthly Activity Reports

Your monthly activity reports should be submitted to the Bursar's Office as soon as possible after month-end. The reports are needed by the 10th of the month at the latest.

Need a little help remembering?

Put a reminder on your calendar for the first of the month (include an alarm).

JUNE REPORTS

At fiscal year-end, offices like to see their sales figures posted quickly. To facilitate that, submit your June activity reports as soon as possible after June 30th.

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@unlnotes.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.

Account Data Compromise

What is an Account Data Compromise? **[Taken from: MasterCard Worldwide's "Why is PCI Important to My Small Business?"]**

An Account Data Compromise is an occurrence that results, either directly or indirectly, in the unauthorized access to or disclosure of payment card account data. This is referred to as a Breach of Security in UNL's Payment Card Policies and Procedures. This can occur with physical receipts, but the most common attacks are targeted at electronic forms of payment card data storage, either internally by a dishonest employee skimming cards or externally through attackers gaining access to the merchant's/service provider's systems from remote locations and subsequently stealing the data.

What do you do if an Account Data Compromise happens or you suspect it may have happened?

Report it immediately at: http://www.unl.edu/helpcenter/

If you suspect loss or theft of any materials containing cardholder data, you must immediately notify the following parties: **1) UNL Police** (402-472-2222), **2) the Bursar's Office** (402-472-1734 or 402-440-2444 after 5:00 pm, and **3) your supervisor.**

May 15th Deadline Approaching for SAQ's

Your completed Self-Assessment Questionnaire (SAQ) is due in the Bursar's Office by ***Tuesday, May 15th***. Version 2.0 will be used for our SAQ again this year. *Thank you to everyone that has already submitted their forms!*

Please refer to our February newsletter for further details on selecting the correct SAQ for your department and completing the SAQ. The SAQ forms and supplemental information are available at:

https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

If you are unsure about any of the compliance questions on the SAQ, please contact:

Mike Rutt
mrutt2@unl.edu or 2-0933

Once the entire form is completed, you will need to print it out. Obtain an appropriate signature for your department in Part 3b of the Attestation of Compliance. Then forward the document to:

Jennifer Hellwege
121 ADMN, 0412
jhellwege2@unl.edu