Payment Cards Processing at UNL

VOLUME 4, ISSUE 2 MAY, 2010

University of Nebraska —Lincoln
Bursar's Office

Good News!

The "Official 4th Quarter 2009-10 PCI Scan" was ran on April 1, 2010

&

We PASSED!

Common Myths of PCI DSS

Taken from "Ten Common Myths of PCI DSS" by the PCI Security Standards Council

MYTH ~ *One vendor & product will make us compliant*

Many vendors offer an array of software and services for PCI compliance. No single vendor or product, however, fully addresses all 12 requirements of PCI DSS. Instead of relying on a single product or vendor, you should implement a holistic security strategy that focuses on the "big picture" related to the intent of PCI DSS requirements.

MYTH ~ *Outsourcing card processing makes us compliant*

Outsourcing simplifies payment card processing but does not provide automatic compliance. Don't forget to address policies and procedures for cardholder transactions and data processing. Your business must protect cardholder data when you receive it, and process charge backs and refunds.

MYTH ~ *PCI compliance is an IT project*

The IT staff implements technical and operational aspects of PCI-related systems, but compliance to the payment brand's programs is **much more than a "project" with a beginning and end – it's an ongoing process of assessment, remediation and reporting.** PCI compliance is a business issue that is best addressed by a multidisciplinary team. The risks of compromise are financial and reputational, so they affect the whole organization. Be sure your business addresses policies and procedures as they apply to the entire card payment acceptance and processing workflow.

MYTH ~ *We don't take enough credit cards to be compliant*

PCI compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one.

MYTH ~ *We completed a SAQ so we're compliant*

. . . a bad system change can make you non-compliant in an instant. True security of cardholder data requires non-stop assessment and remediation to ensure that likelihood of a breach is kept as low as possible.

MYTH ~ *PCI is too hard*

Understanding and implementing the 12 requirements of PCI DSS can seem daunting . . . However, PCI DSS mostly calls for good, basic security. . . . The business risks and ultimate costs of non-compliance, . . . can vastly exceed implementing PCI DSS – such as fines, legal fees, . . . and especially lost business. Implementing PCI DSS should be part of a sound, basic enterprise security strategy, which requires making this activity part of your ongoing business plan and budget.

Fiscal Year End is Nearing

Submit your June activity reports as soon as possible after June 30th. EVERYONE's reports must be submitted before we can post the sales entry.

PCI Data Security Standards Rock

http://www.youtube.com/watch?v=xpfCr4By71U&feature=player_embedded

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.

New Version of PCI DSS is Expected Yet This Year

The Payment Card Industry Data Security Standard (PCI DSS) Version 1.2 was launched October 1, 2008. The lifecycle of the PCI DSS follows a 24-month lifecycle with five stages. We are currently in Stage 4 which began May 1st and goes through August 31st. During this period, a new version is expected to be finalized. In addition to the new PCI DSS, the PCI DSS Council will provide details including phased implementation deadline dates, any subsequent sunset dates, and items affected by the revision update process.

In a Miami Herald article from April 27th, a survey of 155 Qualified Security Assessors identified the following as expected to be included in the new version of the PCI DSS:

> "It is believed that clarifications will be issued on the use of encryption and key management."

> "41% of those surveyed believed tokenization will be included in the update as the technology to use to increase cardholder data security and reduce cost of compliance."

Retention Schedule & Purging of Credit Card Data

Per PCI DSS v1.2, Requirement 9.10.1 "Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed". Cardholder data consists of four items: 1) Primary Account Number (PAN), 2) Cardholder Name, 3) Service Code, and 4) Expiration Date. Items 2, 3, and 4 are only applicable if stored in conjunction with the PAN.

NOTE: Never store the card-validation code or value (i.e. CVV, CVC, CAV, CSC).

University policy states that "Merchants will keep an original or imaged copy of each payment card transaction for no less than 18 months. After 18 months, these must be destroyed in a manner that will render them unreadable.

Discover Now Part of FNMS Contract

We have a limited number of merchants currently accepting Discover as a payment option. The State of Nebraska and First National Merchant Solutions (FNMS) recently finalized an amendment to their contract adding Discover to their processing. This means Discover transactions are now settled through FNMS along with Visa and MasterCard.

Any merchants interested in adding Discover as a payment option can contact Jennifer Hellwege in the Bursar's Office at: 472-9004 or jhellwege@unl.edu She will request this change be made to your merchant account. If you have a terminal, the change would require a new download to the machine. If you are online, the change would require some modifications to your website by your technical staff.