Payment Cards Processing at UNL

VOLUME 5, ISSUE 2 MAY, 2011

University of Nebraska —Lincoln
Bursar's Office

Annual PCI Compliance In Process

The Bursar's Office has received Merchant Profiles and procedures documents from all of the UNL merchants. We are in the process of reviewing this documentation and collecting the SAQs. Please submit your signed and completed SAQ by May 15th if you have not yet done so.

SAQ C-VT is a new category this year and may be applicable to your merchant account. Carefully read all of the qualifications for each SAQ. The SAQ you completed last year may not apply again this year.

Each year it seems that something new comes to light during this review process. We always get some really great questions from merchants.

With the busy schedules each of us maintains, we don't always get the luxury of reviewing processes this regularly. So look at this as the opportunity it is. It's the chance for you to take the time to reflect on your current processes and ensure that they are efficient and yet include the proper internal controls and compliance measures.

Thank you all for your time and efforts in this process!

Fiscal Year End is quickly approaching.

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.

Review your Monthly Merchant Statements

You know your business best. Be sure that all charges are appropriate.

TSYS Merchant Solutions℠

Total System Services, Inc. (TSYS) issued a press release on January 4, 2011 stating, "TSYS Acquires Remaining 49 Percent of First National Merchant Solutions From First National Bank of Omaha." What does this means to us? Our Acquirer, **First National Merchant Solutions (FNMS)**, is now **TSYS Merchant Solutions**.

An email was forwarded March 31st providing information on the changes that occurred with this transition. User IDs and passwords were to remain the same. TSYS Merchant Solutions phone number continues to be 800-228-2443. As expected, names and logos have been updated to reflect the change in ownership. A number of web site address have also reflected these naming changes.

There were some initial issues with the changeover, but we have not heard of any recently. If you experience any difficulties and need assistance, please contact Jennifer Hellwege at 402-472-9004.

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.

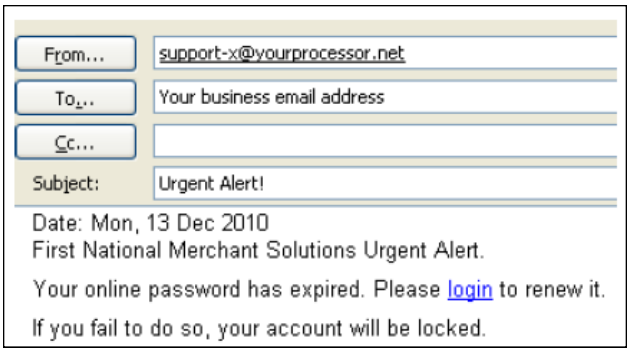
Email "Phishing" Scams on the Rise

Be careful when asked to provide personal information over the phone or through an email. Many of us have received these types of emails personally, and according to Visa, phishing scams directed toward merchants and businesses are increasing.

What is Email "Phishing"? It is an email scam in which criminals attempt to convince a party to provide sensitive information such as merchant account information, passwords, login credentials, PAN, etc. The criminal will send an email that appears to originate from a legitimate financial institution or payment processor (i.e. TSYS or PayPal). Generally, the merchant is asked to click on a link embedded in the email. This link actually connects to the criminal's web site or server and may lead to the installation of malicious software (malware) on the business' computer.

1. **Look Closely at the Sender's Email Address** -The address may include unusual characters or constructs. In the example below, the "-x".
2. **Check Email Images and Graphics** -Images are often broken or out of place.
3. **Pay Attention to Message Format and Text** -Message length, grammar, word choice and sentence structure all play a part. In the example below, the business name is not used to personalize the message. There also is no contact information provided for First National Merchant Solutions.
4. **Pay Attention to Message Tone; Look for Consequences Resulting from Lack of Action** -Does it demand your attention and indicate consequences if you don't take action? This could indicate a fraudulent email.
5. **Consider Whether the Message Received Seems Out of Character** -In the example below, "Why would First National Merchant Solutions send a message like this?"
6. **Be Wary of Embedded Hyperlinks** -Hovering or moving your computer mouse pointer over the embedded hyperlink should reveal the URL. If you don't recognize the URL or if it doesn't match the sender, this may be reason for suspicion. Even links that appear legitimate can have hidden characters or slight modifications. Always open a new browser window and type the web URL into the browser. Do not copy and past the URL included in the email to your browser.

Example of email:



Source: December, 2010 FNMS First Flash