The Office of the State Treasurer has provided details regarding the following:

Credit Card Data Security – Annual PCI Compliance

PCI – Payment Card Industry Compliance Standards and Requirements

Please contact Michelle Raphael [mailto: mraphael@trasurer.org] if you have additional questions regarding these items.

Memorandum from Shane Osborn, State Treasurer re: Deadline for PCI Data Security Compliance Standards and Requirements is Monday, July 7, 2008.

2008 PCI Data Security Compliance Standards Certification form

Press release – February 6, 2008

Press release – February 7, 2008

First Flash – February 12, 2008

STATE OF NEBRASKA

State Treasurer

Shane Osborn
State Treasurer
sosborn@treasurer.org

Suite 2005, State Capitol
Lincoln, NE 68509
402-471-2455, FAX 402-471-4390

Memorandum

To: All Agency Directors for Agencies Who Accept Visa/MasterCard

From: State Treasurer Shane Osborn

RE: **Deadline for PCI Data Security Compliance Standards and Requirements is Monday, July 7, 2008**

Date: February 19, 2008

Dear Agency Director:

If your agency accepts credit card payments, please note the instructions in this memorandum carefully.

The State of Nebraska has remained at a Level 2 Merchant due to transaction volume and now must continue to meet annual Payment Card Industry ("PCI") Data Security Compliance Standards to protect cardholders from fraud and identity theft.

These standards include (1) quarterly scans provided by an approved scanning vendor and (2) an annual PCI Self-assessment Questionnaire. The CIO's Office has requested the applicable PCI Self-assessment Questionnaires be completed at the agency level in order to ensure each individual agency is meeting these PCI Data Compliance Standards.

The DEADLINE for filing your annual PCI SELF-ASSESSMENT QUESTIONNAIRE documentation along with your agency certification letter to the Treasurer is due by Monday, July 7, 2008.

The questionnaire forms recently were changed. A copy of the PCI Security Standards Council press release announcing these changes is attached for your viewing. You may view information about the new PCI DSS forms at https://www.pcisecuritystandards.org/tech/saq.htm .

Instructions on how to complete the required questionnaires and a link to the questionnaires is located at https://www.pcisecuritystandards.org/tech/instructions.htm .

Each agency will only fill in the forms relating to the credit card business services your entity provides as described in the SAQ descriptions for SAQ forms A thru D. Chief Information Security Officer Steve Hartman may require additional data in order to clarify or obtain information to complete the state-wide compliance documentation. **Please go to the links and read the information about the new forms and guidelines.**

Your agency must complete these forms by the deadline! Please note it takes the CIO's Office a significant amount of time to compile and analyze all the data provided by the state agencies.

In order to assist you in completing the PCI Self-assessment Questionnaire, we have set forward **two** dates to meet with representatives from FNMS, the CIO's Office and the Treasurer's Office. Please review and complete as much of your required questionnaires as possible prior to the trainings. Please answer the questions to the best of your ability, and bring any remaining questions to any of the following training sessions:

- Thursday, **May 22, 2008** from 9 a.m. to 11 a.m., RM 1510, State Capitol in Lincoln
- Tuesday, **June 10, 2008** from 9 a.m. to 11 a.m., RM 1510, State Capitol in Lincoln

Agenda for both meetings:

9 a.m. - 9:30 a.m. The focus of the discussion will pertain to state agencies who are utilizing third party vendors (Agencies utilizing Nebraska.gov must attend during this part of the meeting)

9:40 a.m. - 11 a.m. The focus of the discussion will be pertain to all other credit card processing

*Please RSVP your attendance to tmstaff@treasurer.org for the in person meetings. Your agency personnel are invited to attend both meetings. Your agency may send as many staff as you wish to attend the meetings.

*Our office is trying to arrange a call in line for one of the meetings for agencies located too far from the eastern part of the state. Please email tmstaff@treasurer.org if you are interested in participating by phone.

If you cannot attend these training sessions and you cannot complete the applicable PCI Self-assessment questionnaire without assistance, you may contact one of the following for help at your agency's expense.

- Steve Hartman, CISSP
  Chief Information Security Officer
  State of Nebraska
  (402) 471-7031
  Steve.hartman@cio.ne.gov

- Justin Kalhoff, CISSP
  Chief Executive Officer
  Infogressive, Inc
  (402) 429-1091
  justin.kallhoff@infogressive.com

- Lee Pierce
  SecurityMetrics
  (801) 705-5659
  lpierce@securitymetrics.com

Please note: **Failure to complete the applicable questionnaires and to provide certification to the Treasurer's Office can result in our instructions to First National Bank Merchant Services to cease credit card processing for your agency!** If you cannot complete the necessary questionnaires in a timely manner, you must seek assistance from a certified consultant, hire a PCI certified vendor to accept credit cards on behalf of your agency, or refrain from accepting payment cards.

Finally, agency quarterly website scans will need to be completed by ALL agencies including those behind the state firewall each quarter in order to make sure that PCI Data Compliance Standards are met. Please make sure that if your agency is utilizing a Qualified Security Assessor for scanning services that the vendor has remained on the current list of service providers. The list of Qualified Security Assessor is located at: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

All state agencies should be congratulated for the excellent job they did last year when preparing their paperwork during the previous compliance period. We also appreciated your prompt response to phone calls and emails from our staff and Steve Hartman.

Sincerely,

Shane Osborn, Treasurer
State of Nebraska

SO/mr
Enclosures
cc: Michelle Raphael, Director of Treasury Management
Gina Malloy, First National Bank Merchant Services (FNMS)
Steve Harman, State Security Officer, CIO

2008 PCI Data Security Compliance Standards Certification

State Treasurer Osborn:

"Agency" certifies that the PCI Data Security Compliance Standards as required by the Credit Card Associations (Visa, MasterCard, American Express and Discover) have been met.

" Agency" has attached the PCI Self Questionnaire audit report for review by the Treasurer's Office and CIO staff. Our agency has carefully, thoroughly, and truthfully completed a full audit as required and our agency has disclosed any or all PCI concerns/compliance issues. Our agency has also reviewed our security procedures and policies that pertain to PCI Compliance.

"Agency" certifies that all scans have been performed by a Qualified Security Assessor PCI Scanning Vendor and I have verified that the scanning entities name is on the Visa and MasterCard Association list.

"Agency" understands that Cardholder Data is any personally identifiable data associated with a cardholder. This could be identified as an account number, expiration date, name, address, social security number, etc. I certify that all forms and merchant slips received by our agency containing cardholder data is stored in a locked/secured cabinet with limited access granted only to authorized state agency personnel.

"Agency" certifies that our computer servers, switches, and equipment storing credit card data are located in a secured area/room within our agency that has limited access to authorized agency personnel only.

"Agency" certifies that any service related to credit card processing that is outsourced to a third party vendor, that the vendor is compliant with PCI DSS requirements. I understand it is my responsibility to verify this compliance remains current during the term of services with the third party vendor. I understand that the following two paragraphs also apply if my agency has hired the third party vendor for credit card services.

"Agency" understands that if a security breach or compromise of data occurs, the **"Agency"** is required to **immediately** disclose this information to the State Credit Card Merchant Bank, the State Treasurer's Office, the State of Nebraska CIO's Office, the FBI, the Nebraska State Patrol and other law enforcement (as directed by the CIO's and Treasurer's Office). **"Agency"** understands that if breach or data compromise is not reported immediately, **"Agency"** will be responsible for the additional Card Association fines.

"Agency" accepts any and all financial liability for any cardholder data compromised including but not limited to: any fines/penalties or punitive damages charged by the Card Associations, costs (if charged) incurred by law enforcement, the State of Nebraska CIO's Office, the State Treasurer's Office, and the company hired to complete the forensic scan and assist in the investigation. I understand that any and all additional costs incurred due to a breach of any type will be the responsibility of my office.

_____
Signature - Agency Director

_____
Printed Name – Agency Director

_____
Printed State Agency Name **"Agency"**

_____
Date

PRESS RELEASE

Payment Card Industry
Security Standards Council, LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

Media Contacts

Glenn R. Boyet	Ella Nevill or Matthew Mors
PCI Security Standards Council	Text 100 Public Relations
+1 (617) 876-6248	+1 (212) 331-8410 (Eastern U.S.) +1 (206) 267-2004 (Western U.S.)
gboyet@pcisecuritystandards.org	pci@text100.com

FOR IMMEDIATE RELEASE

PCI SECURITY STANDARDS COUNCIL ISSUES UPDATED SELF ASSESSMENT QUESTIONNAIRE

—Enhanced validation tool helps merchants protect their payment data—

WAKEFIELD, Mass., Feb. 6, 2008 — The PCI Security Standards Council, a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (DSS), PCI PIN Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS), today announced that its updated Self Assessment Questionnaire (SAQ) for merchants and service providers is now available.

The SAQ is an important validation tool primarily used by merchants and service providers to demonstrate compliance with the PCI DSS. This new SAQ is specifically designed to simplify and streamline the assessment process and aid merchants who are not required to have onsite assessment to protect payment card data. "With the introduction of the updated SAQ, merchants will now have a better understanding of the steps necessary to secure their payment data and comply with the PCI DSS," said Bob Russo, general manager, PCI Security Standards Council.

Underscoring the need for continued adoption of the PCI DSS by merchants is a recent report by Javelin Research and Strategy in which 63 percent of consumers believe that merchants and retailers are the least secure among payment transaction stakeholders in protecting account information. [1]

In response to industry feedback, this new SAQ incorporates updates designed to reflect the most recent version 1.1 of the DSS and replaces an earlier version that had been in place since January 2005. The SAQ, version 1.1 is now available at https://www.pcisecuritystandards.org/tech/saq.htm and consists of four unique forms to meet various business scenarios. These four include:

- SAQ A: Addresses requirements applicable to merchants who have outsourced all cardholder data storage, processing and transmission.

[1] Cundiff, Bruce. "Data Breaches and Buyer Behavior: Moving PCI Compliance from Costly Burden to Competitive Advantage," Javelin Strategy and Research, March 2007.

—more—

- SAQ B: Created to address requirements pertinent to merchants who process cardholder data via imprint machines or standalone dial-up terminals only.
- SAQ C: Constructed to focus on requirements applicable to merchants whose payment applications systems are connected to the Internet.
- SAQ D: Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under the types addressed by SAQ A, B or C.

Also included on the Council's Website is a set of frequently asked questions and an instruction and guideline document for the SAQ, intended to simplify the process and ensure that merchants and service providers can more easily determine which SAQ is the proper tool for them to use in confirming PCI DSS compliance.

"Issuing the latest self assessment questionnaire is another step the PCI Security Standards Council is taking to ensure that all merchants and service providers have options in determining their compliance strategy," said Russo. "Having multiple SAQs available will streamline the process and make it easier for stakeholders to determine their compliance gaps and take action to ensure full compliance with the Standard."

For More Information:

If you would like more information about the PCI Security Standards Council or would like to become a Participating Organization please visit pcisecuritystandards.org, or contact the PCI Security Standards Council at info@pcisecuritystandards.org.

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of the PCI Data Security Standard (DSS), PIN Entry Device (PED) Security Requirements and the Payment Applications Data Security Standard (PA-DSS). Merchants, banks, processors and point of sale vendors are encouraged to join as Participating Organizations.

###

PRESS RELEASE

Payment Card Industry
Security Standards Council, LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

Media Contacts

Glenn R. Boyet	Ella Nevill or Matthew Mors
PCI Security Standards Council	Text 100 Public Relations
+1 (617) 876-6248	+1 (212) 331-8410 (Eastern U.S.) +1 (206) 267-2004 (Western U.S.)
gboyet@pcisecuritystandards.org	pci@text100.com

PCI SECURITY STANDARDS COUNCIL TO HOST WEBINAR ON LATEST SELF ASSESSMENT QUESTIONNAIRE

—Merchants and service providers to gain insight into latest tool for PCI self assessment—

WAKEFIELD, Mass., Feb. 7, 2008 — The PCI Security Standards Council, a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (DSS), PCI PIN Entry Device (PED) Security Requirements and the Payment Application Data Security Standard (PA-DSS), today announces a complimentary webinar, "Navigating and Understanding the PCI SSC Self Assessment Questionnaire," to be held on Thursday Feb. 21, 2008 at 11:30 a.m. EST and a second session the same day at 7:30 p.m. EST.

The new Self Assessment Questionnaire (SAQ), announced on Feb. 6 2008, is an important validation tool primarily used by merchants and service providers to demonstrate compliance with the PCI DSS. This new SAQ is specifically designed to simplify and streamline the assessment process and aid merchants who are not required to have an onsite assessment to protect payment card data. This educational webinar, featuring Bob Russo, General Manager, and PCI SSC's chair of the Technical Working Group, Lauren Holloway, who will address the different SAQ forms and scenarios to help merchants and service providers with their PCI assessment programs.

Webinar participants will discover:

- The role of the SAQ and its alignment with the latest PCI DSS;
- The new forms and documents that are based on unique business scenarios;
- The process flow for determining which SAQ fits your unique needs, and;
- How to maximize the use of the new SAQ web pages on the Council's website.

To register for the Thursday Feb. 21, 2008 at 11:30 a.m. EST session, visit http://www.webcastgroup.com/client/start.asp?wid=0780221083975 or http://www.webcastgroup.com/client/start.asp?wid=0780221083976 for the 7:30 p.m. EST session.

—more—

For More Information:

If you would like more information about the PCI Security Standards Council or would like to become a Participating Organization please visit pcisecuritystandards.org, or contact the PCI Security Standards Council at info@pcisecuritystandards.org.

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of the PCI Data Security Standard (DSS), PIN Entry Device (PED) Security Requirements and the Payment Applications Data Security Standard (PA-DSS). Merchants, banks, processors and point of sale vendors are encouraged to join as Participating Organizations.

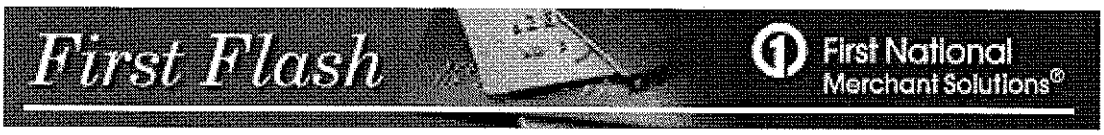
###

Michelle Raphael

From: Molloy, Gina [gmolloy@fnni.com]
Sent: Tuesday, February 12, 2008 12:10 PM
To: Michelle Raphael
Subject: RE: First Flash Visa Rate Notification and PCI DSS Updates
Attachments: 02-06-08_NEW SAQ Info from PCI DSS.pdf; New SAQ Webinar.pdf

---

From: First National Merchant Solutions [mailto:FirstNationalMerchantSolutions@fnni.com]
Sent: Tuesday, February 12, 2008 7:54 AM
To: First National Merchant Solutions Processing Clients
Subject: First Flash Visa Rate Notification and PCI DSS Updates



First Flash

First National Merchant Solutions is providing you with the following changes which may impact your business:

ISA Fee Update
Visa has made changes to the International Service Assessment charge effective April 1, 2008. First National Merchant Solutions notified you of this new fee in a First Flash sent on November 13, 2007 and in the Regulatory Summary sent in January and February.

Visa introduced the International Service Assessment fee as 0.15% on transactions processed by a business in the U.S. when the card is issued outside of the U.S.

Visa has increased the rate on the International Service Assessment fee from 0.15% to 0.40%. This fee applies to every $1.00 in transactions made at a U.S. location on cards issued outside of the U.S.

If you provide cash advances (Applies to Banks only)
Visa will assess a new ISA rate of 0.15% on cash advances processed at a business when the card was issued outside of the country the transaction is accepted in.

New PCI DSS Questionnaires Released
The PCI Security Standards Council has updated the Self Assessment Questionnaire (SAQ) for merchants and service providers. The questionnaire is part of the requirements businesses must fulfill in order to achieve compliance with the Payment Card industry Data Security Standards (PCI DSS). The updated SAQs are geared toward methods used to capture cardholder data at the point of sale and in transmission. For instance,

- If you outsource all cardholder data storage, processing and transmission, you would complete SAQ A
- If you process transactions via a dial terminal or manual imprint machine, you would complete SAQ B
- If you process transactions on the Internet, you would complete SAQ C
- If you do not fall under A, B, or C, you would use SAQ D

Visa Expands ADCR
Visa has expanded the scope of the Account Data Compromise Recovery (ADCR) process to include violations of the Payment Card Industry (PCI) Data Security Standard (DSS) requirements that could allow a compromise of full magnetic-stripe data. Prior to this change ADCR was limited to compromises involving storage of magnetic-stripe data.

These revisions are effective for qualifying Compromised Account Management System (CAMS) alerts that occur on or after January 22, 2008. For more information, contact your national account manager.

First National Merchant Solutions - the payment processor you rely on for service and stability