

MICHIGAN STATE UNIVERSITY

DATE: July 16, 2010

TO: Deans, Directors, Chairpersons and Executive Managers

FROM: David Brower and David Gift

SUBJECT: SECURING DATA ENTRY AND COMPLIANCE WITH PCI DSS

All Units that accept payment (credit/debit) cards (subsequently referred to as Merchants) must comply with the Payment Card Industry Data Security Standard (PCI DSS). The purpose of this memo is to alert Merchants to a new interpretation of the PCI DSS that may require changes to how they do payment processing to remain compliant.

Who is Impacted

This new interpretation applies to all Merchants with staff who enter card data on behalf of a customer into any Internet connected device (e.g., personal computer or workstation). This includes all Merchants that use the manual entry feature of *webCredit*, as well as its replacement, *CASHNet*, and any other third party application. This does not affect those Merchants who use only a swipe terminal or those Merchants whose customers always enter their own card data on their own computers, such as tuition payments made via *StuInfo*.



OFFICE OF THE CONTROLLER

Hannah Administration Bldg
426 Auditorium Rd Rm 305
East Lansing, MI
48824

517-355-5020
FAX: 517-432-5269
<http://ctrl.msu.edu>

Retaining Compliance

MSU was previously advised that using a workstation for entering card data on behalf of a customer into a PCI validated payment application was compliant. Due to evolving technology and ever-changing security issues, MSU is now being advised that **entering card data into a general-use workstation is not compliant**. To be compliant, each Merchant has three basic options: switch to a swipe terminal, reconfigure and dedicate the workstation as defined below, or require customers to enter card data on their own behalf (i.e., stop taking phone/mail orders).

Dedicated Workstation

The PCI DSS requires any workstation supported by a Merchant for the purpose of entering card data to have:

- **Limited Use** – the workstation must be configured to only allow access to those applications necessary to process the card transaction. The workstation cannot allow email or open Internet surfing. Neither can it have word processing, spreadsheet, instant messaging or similar applications installed. USB ports except for keyboard/mouse need to be disabled or blocked.

- **Firewall** – the workstation must have a hardware firewall device between it and any network to which it is attached. Contact ATS for firewall specifications at <http://help.msu.edu/>.
- **Scans** – the workstation and firewall must have quarterly vulnerability scans. This requires the workstation and firewall to have fixed IP addresses. Contact Mary Nelson at nelsonm@msu.edu or 355-5023, extension 150, to request access to the scanning application.

Note: All Internet-connected devices provided by the Merchant, whether used on- or off-campus at a conference or event, or offered to customers for entering their own card data (e.g., kiosk) must be a dedicated workstation.

Action Required

Each Merchant must **act immediately** to switch to a swipe terminal, create a properly configured dedicated workstation, or discontinue entering card data on behalf of customers. Merchants opting to use a dedicated workstation may have one per staff member or one that is shared (older, used equipment may be an option if it is properly secured). Merchants must provide alternate methods for staff members to access email and other web-based employee services. The PCI Team will distribute more information to existing Merchants. Merchants with a more complex card processing environment and a business need that may entail other options should contact Mary Nelson for additional information.

Summary

We recognize that this requirement will impact Merchants differentially, and depending on the options chosen, some more significantly than others. However, as security threats expand, it is necessary for the card processing culture to adapt. We know from past experience that a breach at one Merchant can directly impact the entire University. Your immediate attention to this matter is required and appreciated.