Overview

This PCI training is required for University employees who are involved in credit card processing. It is the department's responsibility to make sure employees working with credit cards are trained on a yearly basis.

Please review the screens for each type of processing you use. This training is recommended for workers who are working as cashiers and accepting credit cards.

After reviewing the lesson and answering the Quiz, reply in the text with your department and quiz answers.

- Employees who work with credit cards need do this training.
- PCI-DSS stands for Payment Card Industry Data Security Standards and is intended to protect customers against fraud and identity theft.
- PCI is mandated by the credit card companies and if we do not follow these standards the University could be fined along with bad publicity.
- The University IT and Business Services departments oversees PCI Compliance. Please see the Business Services website for PCI and Safeguarding Customer Information.
- PCI compliance must be renewed by the University every year. MSUB's renewal date is January 1. MSUB employees who work with credit cards are required to complete training and review documentation on business processes on a yearly basis.
- Overview of PCI DSS requirements: https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf

Departments/cashiers/student employees who work with credit cards using VX570's, a POS system or other method of acceptance:

- The machines should be settled every night after closing.
- Do not allow anyone to inspect or remove the machine unless you know who they are.
• If your machine appears to have been tampered with, please contact the Business Services Director, CIO, or the Administrative Services Vice Chancellor. The directors and/or Vice Chancellor will determine whether or not the MSUB Police needs to be contacted.

• Cashiers and all other MSUB employees working with credit cards should read the policies and procedures for Safeguarding Customer Information and Cash Account and Deposits. [http://www.msubillings.edu/boffice/Policy%20&%20Procedures.htm](http://www.msubillings.edu/boffice/Policy%20&%20Procedures.htm)

• Refund questions and refunds needing to be processed should be directed to the Business Services Director. Please include date, card type, transaction amount and the last four digits of the credit card number.

• If you are hand entering credit card numbers, do not accept credit card numbers taken through e-mail (phone, analog fax and US mail are okay as long as the credit card number is kept secure until entered and destroyed afterwards). Fax machines connected to the network should not be accepting credit card numbers.

• If a credit card is denied, do NOT override under any circumstances.

• Do not accept a credit card if the signatures do not match or another picture ID with a name does not match the name on the credit card, the card appears to have been altered or tampered with, the embossing on the card is illegible, the card doesn't have an expiration date, the hologram is not clear, the picture in the hologram does not move, or a message comes up when the card is swiped to "pick up" the card. Cards should also not be accepted if the card does not belong to the cardholder.

• Visa cards begin with a 4, MasterCard starts with a 5, and Discover starts with a 6. Do not accept a credit card with a number that does not correspond to the credit card type.

• Requirements for PCI compliance include:
  Keeping all credit card information (card number, expiration date, verification code) secure until processed and destroying immediately afterwards.
  Never sending or accepting cardholder data via the internet (e-mail, networked fax, spreadsheet attachment in e-mail).
  Access to cardholder data is limited to only those individuals whose jobs require such access.
  Equipment is inspected periodically to make sure the devices have not been tampered with.

• The Square and other card readers that attach to systems (laptops, cell phones, iPads, etc.) are not approved.

• Please review:
  [https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf](https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf)
Departments with a NelNet, T2, AceWare, MyOnlineCamp, Insight, CollegeNet, StarRez, MBS and/or MyLearningPlan websites that credit card numbers are only accepted through the site:

- Best practice is to not hand enter a credit card number for a customer into your site using your office computer. Do not offer your computer to a student to enter their credit card information.
- Computers may not be set out for customers to make payments at a location unless they have been provided by IT.
- MSUB employees working with credit cards, cashiers and student workers are required to review this PCI training annually.
- You may process your own refunds through the website and you do not need the credit card number. Contact the Business Services Director if you have questions.
- Do not give your website password(s) to anyone else. Any new person allowed access to the system is required to take the credit card training.
- All websites taking credit card payments for conferences, registration, or events need to have prior approval from Business Services.

Departments who accept credit cards through 3rd party software or 3rd party vendors:

- All 3rd party vendors need to be PCI compliant and they are responsible for the security of the credit card numbers.
- If an outside vendor is coming in with their own credit card machine (for example a company who is doing background checks for the students), they must receive permission from IT to connect to the MSUB computer network.
- All contracts related to software and credit card compliance must include PCI compliance and must be approved by the CIO and the Business Services Director.
Breach Information

If you think that you've had a compromise/breach (for example, a locked cabinet with full credit card numbers ready for processing was broken into), please contact the Business Services Director, CIO, or the Administrative Services Vice Chancellor. They will make the determination on who else should be contacted, ie. University Police, Visa, the local FBI, and/or U.S. Secret Service. Fines for non-compliance violations range from $5000 to $100,000 per month based on credit card volume and number of violations.

Recent Breaches:

January 10, 2013

Texas Southern University's radio station KTSU gave a volunteer position to a person with a criminal history of credit card fraud. The volunteer was later arrested for allegedly using the radio station's donation drive to steal credit card information. The dishonest volunteer faces up to 300 counts of credit card fraud for attempting to use the information on donor pledge sheets.

December 11, 2013

A cyber attack caused the information of clients associated with the L.A. Gay and Lesbian Center to be affected between September 17, 2013 and November 8, 2013. Names, Social Security numbers, credit card information, dates of birth, contact information, medical information, and health insurance account numbers may have been exposed.

October 11, 2013

A data management firm discovered that Chrome browser users may have had their personal information stored on the hard drives of their computers without their knowledge or consent. Google Chrome regularly stores names, street addresses, email addresses, phone numbers, bank account numbers, credit card numbers, and Social Security numbers in web browsers for later use. It was not known that Chrome's cache also stores the information in plain text.

February 19, 2014

Hackers gained access to Social Security numbers, dates of birth and names for more than 300,000 people who attended or worked at the University of Maryland. The breach affected 309,079 people who had received a university identification card since 1998.

December 12, 2014

The University of California Berkeley has notified individuals of a data breach in their Real Estate Division that resulted in unauthorized access to servers used to support a number of Real Estate programs and work stations. The investigation of the hacking showed that these servers were breached in mid-to late September. The personal information included names, Social Security Numbers, credit card numbers and driver's license numbers.
General Reminders:

1. Do not store full credit card numbers anywhere.
2. Double check old forms on file, old receipts, etc. Destroy the credit card number. It is okay to throw away old credit card receipts with full credit card numbers - PCI requirements override record retention requirements.
3. Double check to make sure there are no Social Security numbers on old forms or stored in your computer. Do not post or display SSNs or transmit over the internet.
4. Limit access to personal information as much as possible.
5. Be sure to change passwords on a regular basis and never use default passwords.
6. Secure customer records and information by locking rooms and file cabinets.
7. Make sure any employee in your department who will be working with credit cards takes this training.

QUIZ:

1. All suspected breaches should be reported to:
   a. Business Services Director
   b. CIO
   c. Administrative Vice Chancellor
   d. At the least one of the above

2. Can credit card numbers be accepted via email:
   a. Yes
   b. No

3. How often should PCI training be accomplished:
   a. Weekly
   b. Monthly
   c. Semi-annually
   d. Annually

4. Credit Card fraud can turn a person’s life upside down. Do you feel that this training and protecting credit card information is important:
   a. Yes
   b. No

Submission of Training:

Please reply to this email and include your department and quiz answers in the text. Please print this training and have it handy for reference. jnielsen@msubillings.edu