Part I – Introduction
  – What is PCI-DSS?
  – Why you are here?

Part II – PCI DSS at NU
  – PCI requirements for Higher Education
  – PCI requirements for NU Merchants

Part III – Protecting Sensitive Credit Card Data
  – Your Role
  – Types of Data Breaches and How to Prevent Them
  – Preventing Fraud

Sources for More Information
Introduction
The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

PCI DSS 2.0 (latest version) published 10/28/10; effective for 3 years starting 1/1/2011
Why you are here?

- You and/or people you manage have access to credit card data
- PCI DSS requires that employees be educated at least annually on the importance of credit card security
- NU Merchant Card Policy requires that at least one representative from each Merchant attends centralized PCI-related security awareness training annually
  - Other merchant employees may attend centralized training or separate training may be provided in accordance with this content
Part Two

PCI DSS at NU
PCI Requirements for Higher Ed

- Compliance reported to processor as a Level 3 merchant
  - NU’s annual e-Commerce transaction volume is over 20,000 across all card types.
  - We need to be compliant at all times; FDMS/Citi monitors our SAQs and vulnerability scans via TrustKeeper

- If a breach occurs, we could be raised to Level 1
  - Increased scrutiny from bank and PCI
  - Formal investigations and on-site audits
  - Possibility of losing approval to process credit cards
  - High financial and reputation costs for the University, including potential impact on access to grants/funding
Every merchant department must handle credit card information in accordance with the PCI standards at all times.

Every merchant department must validate compliance annually.

Departments will lose ability to process credit cards if not compliant.
Part Three

Protecting Sensitive Credit Card Data
PCI DSS compliance largely depends on the people who
- select and implement merchant systems,
- select the equipment and
- set department policies

However...

Anyone with access to sensitive data has the ability to prevent or enable data breaches

You have the responsibility to protect data with which you are entrusted
Common Types of Data Breaches

- Technology Attacks
  - Hacking

- Lost or stolen equipment
  - Laptops, USB drives, disks

- Stolen or copied paper records

- Inadvertent disclosure

- Malicious Insiders
Each user needs own ID with strong password
- IDs need to be disabled when no longer needed

Lock or log-off from computer terminals that process credit card data when not in use

Prevent credit card terminals or credit card processing computers from physical access by unauthorized persons
Protecting Data Storage Devices

- Do not create spreadsheets or documents to store credit card numbers, or otherwise store any sensitive credit card information electronically on university equipment.

- Notify supervisor immediately if you receive full credit card numbers electronically from any university source.

- Lock equipment out of sight when not in use.
Your IT guys are your friends!

- Let your supervisor and IT people know that you process credit card data so that they can ensure your computer is protected
- Immediately tell them if you notice strange behavior on your computer, or if unexpected software is running
- When equipment is due to be replaced, sold, or discarded, remind them it was used to process credit card numbers
Avoid creating paper records whenever possible (i.e. don’t print unless necessary).

Never collect CVV2/CID/CSC on paper forms

Lock up papers containing credit card data when not in use.

Destroy papers using an approved shredder. Do not put paper containing intact credit card data in the regular trash.
Preventing Inadvertent Disclosure

- Do not email or instant message sensitive data including credit card numbers
- Question anything that seems to contain unnecessary sensitive data
- Follow the guidelines for protecting data storage devices and paper records
Preventing Fraud

- Refund fraud attempts have been seen at NU
  - Policy requires supervisor approval for refunds

- Refunds must be applied back to the same card originally charged

- Refund amount must be less than or equal to charge

- Monitored by both NU and processor
Notify a supervisor or manager if someone appears to be using sensitive data inappropriately, or if sensitive information is found where it shouldn’t be.

Remember…

- PCI-DSS requires security screening for employees, particularly those with access to multiple credit card numbers at one time.
- NU requires background checks for new employees who will handle credit cards.
Don’t betray your customers’ trust:

Protect every credit card number as though it were your own.

The size of the breach doesn’t matter if your card number is lost.
Merchant Card Program Updates
Merchant Card Program Updates (cont)

- **New processor – FDMS (First Data Merchant Services)**
  - Contract was executed in September, 2010
  - All locations completely transitioned as of July, 2011
  - Discount/fee structure more competitive

- **Terminals**
  - Omni 3200SE obsolete as of 9/2011; although still functioning in some cases, will no longer be supported
  - Contact ccard program to order a new terminal at Ccard@northwestern.edu w/subject line “New Terminal Request”
If you suspect a credit card data breach

- Contact Martin Soler
  - (847) 491-5382

- Follow NU’s Incident Response Protocol
  - http://www.it.northwestern.edu/policies/incident.html
Sources for more information

- PCI Security Standards Council
  - https://www.pcisecuritystandards.org/

- NU Merchant Card Policy and Related Documents