

Path to Compliance

PCI DSS at Tufts University

The Treasury Institute for Higher Education

PCI-DSS Workshop May 6, 2008

Donna Reilly - Tufts University, Treasury Operations

Deborah Nanni – Tufts University Information Technology

Tracy Filosa - TAF Consulting

Effective Commerce



THE NEW YORKER



"You know, you can do this just as easily online."

Martin Luther King Jr.'s Birthday (observed) (USA)

MONDAY
JANUARY 21

Agenda

- About Tufts
- PCI DSS Introduction and Response
- Functional Strategy
- Technical Stewardship
- Tufts PCI Standards and Procedures
- Communication and Outreach
- Ongoing Compliance Process

About Tufts University



- Private university established 1852
- 3 campuses in the Boston-area; 1 international campus
- 9,000 full-time and 1,000 part-time students
- 12 undergraduate and graduate schools including Medical, Dental, Veterinary and Nutrition
- Multiple programs abroad
- 4,100 faculty and staff
- \$2 billion in assets of which 70% is in investments and cash

Business at Tufts

- All financial processes are centrally managed
- Some IT resources are managed by central IT, but deployment decentralized at school-level
- 40+ merchant departments and growing
- 125,000 annual transactions and growing
- Processing methods: card present, MOTO, web forms, virtual terminals, eCommerce
- Central Administration pays for most credit card and eCommerce-related fees

PCI DSS Introduction and Response

- Server processing credit card information breached in 2005
- Deemed Level 1 by acquirer
- VPs of Finance and IT sponsored joint task force consisting of Treasury and IT personnel
- Engaged services of QSA
- Engaged consultant to support project management, documentation and outreach
- Project goal: University compliance and PCI DSS certification

PCI DSS Introduction and Response: Discovery Process

- Searched web sites
- Inquired about servers
- Reviewed service and software providers' contracts
- Searched files and archives that contain credit card information
- Identified and reined in the rogue processors

PCI DSS Introduction and Response: Critical Decisions

Two critical policy decisions were made that lay the cornerstone of the project:

- Tufts would not allow the storage of any complete credit card data on any University owned/controlled computers, servers, desktops, laptops, disks, flash drives, etc.
- All eCommerce must be conducted by using the University's "Authorized Vendor"

Functional Strategy: Get Hosted

- Select an Authorized Vendor to provide exclusive hosted payment gateway services
 - Identified potential eCommerce business partners
 - Issued RFP
 - Involved cross selection of departments in the selection process: Treasury, Finance, UIT, Bursar, Clinics, Advancement
- Convert existing online commerce to Authorized Vendor
- Implement all new eCommerce via Authorized Vendor

Functional Strategy: Develop Policy

University Policy for Accepting Credit Card and eCommerce Payments

- Background and applicability
- Implementation process
- Define roles and responsibilities, MDRP
- Process for responding to security breach
- Links to additional information

Functional Strategy: Formalize Procedures

Create “Application to Become a Merchant Department”

- Purpose of business, revenue and economic benefits expected from accepting credit card payments
- Third parties/software packages that will be involved in the processing of credit cards.
- Designate the MDRP
- Required approvals of Department Manager and school’s Budget and Fiscal Officer
- Signatures acknowledge that have read and understand the University Policy, role and responsibilities

Technical Stewardship

- Liaison with technical and assessor staff
- Identify systems to scan and/or shut down
- Coordinate quarterly scans and annual penetration
- Renegotiate contracts with addendums stipulating the need to adhere to the PCI DSS requirements
- Investigate and determine best practices for proper disposal of materials containing credit card and personal data

Tufts University Payment Card Information Standards and Procedures

Draft Standards and Procedures for Certification

- Purchased template
- Tracks PCI Audit Standards
- Tool to control scope

Communication and Outreach: Communicating at All Levels

Executive Administrative Deans



University-wide Newsletter

Getting the Word Out

University Finance

New policy on safeguarding your credit card information



Left to right,
Deborah Nanni,
Darlene Karp, and
Donna Reilly

OVER THE PAST SEVERAL YEARS, more and more Tufts departments have been accepting credit card and electronic payments. Credit cards, and the Internet in particular, enable efficient and convenient payments for goods, services and gifts. However, recent news reports of security breaches, credit card fraud and identity theft drive home the threats associated with these payments.

Tufts is taking action to secure the credit card and personal information of its customers and supporters:

- The University has implemented the new Policy for Accepting Credit Card and eCommerce Payments, which describes the responsibilities of the University and departments regarding accepting credit card and eCommerce payments. Anyone considering credit card processing should read this policy. Departments must register with Treasury Operations before accepting any credit card or eCommerce payments.
- A core project team of Darleen Karp and Donna Reilly of Treasury Operations and Deborah Nanni

of University Information Technology is coordinating the University's efforts to comply with requirements, launch secure internet commerce and protect sensitive information.

- The University has selected an "Authorized Vendor" to host all of the University's web payment gateways and to process electronic credit card and bank payments. The hosted environment enables secure eCommerce that is integrated with Tufts' websites and administrative systems. This exclusive relationship also enables the University and departments to leverage the volume of eCommerce transactions and reduce processing costs.

Over the next few months the project team will be offering information sessions and targeted training programs for employees who process credit card information and conduct eCommerce. Cash Manager Reilly adds, "We will also continue to work closely with each merchant department to develop a credit card and eCommerce solution that meets their business needs and protects the University, its customers and supporters."

To read more about the new policy and resources go to: <http://finance.tufts.edu/treasury/> or contact Donna Reilly at treasury@elist.tufts.edu or 7-3266.

Communication and Outreach: Merchant Department Handbook

- University Policies related to credit card processing
- 12 standards of the PCI DSS
- Roles and Responsibilities
- Chargeback process
- Contact information - equipment, troubleshooting, supplies
- Breach or suspected breach instructions
- Forms for annual compliance:
 - Self Assessment Questionnaire
 - Annual Merchant Department Employee Terms of Use Agreement

Communication and Outreach: Merchant Department Handbook Sample Pages

Merchant Department Responsible Person (MDRP)

If you are an MDRP



Don't Forget...

You are ultimately responsible for the secure processing of all credit card and eCommerce payments for your department. This means your responsibilities include:

- Ensuring all credit card processing equipment is secure and only accessible to those who have been approved to participate in processing these payments
- Becoming familiar with all relevant University policies and making sure your department is complying with these guidelines when accepting credit card and eCommerce payments.
- Educating others so they are aware of your department's responsibilities and able to protect customers' personal payment information.

Attestation of Compliance, SAQ B

Instructions for Submission

The Merchant Department must complete this Attestation of Compliance as a declaration of the merchant's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and refer to the submission instruction at "PCI DSS Compliance - Completion Steps" in this document.

Tufts University Merchant Department Information

Department: [REDACTED]	Merchant ID: [REDACTED]
MDRP: [REDACTED]	MDRP Title: [REDACTED]
MDRP reports to: [REDACTED]	Supervisor Title: [REDACTED]
Campus phone: [REDACTED]	Email: [REDACTED]
Campus address: [REDACTED]	
URL: [REDACTED]	



Protecting Cardholder Data

1. Only grant access to credit card and electronic payment data, as well as processing equipment to those with a business need-to-know.
2. Never use email to transmit complete credit card or personal payment information.

Communication and Outreach: Training Sessions/Site Visits

Training sessions/site visits with merchant departments:

- Required attendance for all MDRPs
- Delivered and referenced MD Handbook
- Introduction to PCI DSS and University's efforts
- Established cooperative working relationships
- Discovery and problem solving

Communication and Outreach: Internal Documentation

Treasury and UIT PCI DSS Manual

- Explicit instructions for credit card and eCommerce processes
- Breach roles, responsibilities and tasks
- Contact information

Ongoing Compliance Process

Quarterly:

- Continue scanning servers until brought offline

Annually:

- Staff Handling Credit Card Data: complete the “Tufts Merchant Department Annual Employee Terms of Use Agreement”
- Merchant Department-complete the appropriate SAQ as determined by Treasury Office
- Conduct Penetration Test
- Treasury- compiles all SAQs and submits University SAQ to acquirer-updates handbook as needed

Thank you

Donna Reilly

Cash Manager

Tufts University Treasury Operations

donna.reilly@tufts.edu

Debbie Nanni

Special Projects Manager

Tufts University Information Technology

Deborah.nanni@tufts.edu

Tracy Filosa

Principal

TAF Consulting

tfilosa@tafconsulting.com