NORTHWESTERN
UNIVERSITY

# Merchant Card Processing Policy

## Table of Contents Page#

NORTHWESTERN
UNIVERSITY

**Responsible University Official:** Ingrid Stafford
**Responsible Office:** Treasury Operations
**Origination Date:** July 8, 2008

# MERCHANT CARD PROCESSING POLICY

## Policy Statement

In order to accept credit or debit card payments, a Northwestern University (NU) school, department, or organization must:

- receive prior permission from e-Commerce Operations within Treasury Operations, and
- ensure that the payment process and related recordkeeping adhere to university accounting guidelines, the Payment Card Industry Data Security Standard (PCI DSS), and all applicable legislation.

## Reasons for Policy/Purpose

1. Merchant credit or debit card transactions are monetary transactions and are subject to the same control and reconciliation policies as cash transactions.
2. Merchant card transactions are governed by university-wide banking agreements; therefore, independent establishment of payment processes may constitute a breach of contract.
3. Improper protection of merchant card data, whether in electronic or paper form, could lead to a security breach that may result in
    - customer ill-will,
    - damage to NU's reputation,
    - fines,
    - legal fees,
    - notification-related costs, and
    - concessionary costs, such as offering credit monitoring to individuals put at risk.

    Potential ramifications of a data breach are greater if the merchant is not in compliance with the minimum security standards required by the payment card industry (PCI DSS).

## Who Approved This Policy

Ingrid Stafford

## Who Needs to Know This Policy

Any NU employee, contractor, business partner, or student involved in the processing of debit and credit card payments or who has authority over a system that accepts such payments.

## Website Address for this Policy

http://www.northwestern.edu/controller/treasury-operations/e-commerce-operations/index.html

## Contacts

If you have any questions on the policy or procedure for Merchant Card Processing, you may contact e-Commerce Operations via an email to Ccard@northwestern.edu.

## Definitions

| | |
|---|---|
| e-Commerce | The process of conducting payment transactions over a computer network, usually the Internet. In e-commerce the merchant card is usually not present; instead, the payer enters that data into a web-based form remotely. |
| e-Merchant | A merchant who uses an e-commerce system to generate revenue. |
| Merchant | A department, school, or other NU organization that collects revenue. Although merchants may receive payments in various forms (i.e. cash, check, voucher) this policy applies to merchants who wish to receive at least some of their payments from credit or debit card transactions. |
| Merchant Card | Debit or credit cards, including those under the Visa, MasterCard, Discover Card and American Express brands. |
| Merchant ID | A merchant identification code assigned by the bank and is used to identify the owner of merchant card transactions. |

| | |
|---|---|
| PCI DSS | The Payment Card Industry Data Security Standard (PCI DSS), currently PCI DSS v2.0, defines security requirements for card transactions and is required by a consortium of card providers (i.e. Visa, Master Card, Discover, and American Express). Failure to comply with PCI DSS may result in substantial fines and increased auditing requirements if a breach occurs. The full text of the standard and other supporting documents are available at https://www.pcisecuritystandards.org/. |
| Payment Card | See "Merchant Card." |
| POS System | Point-of-Sale system. A computer-based system that processes payments over a network. A POS system differs from an e-commerce system in that the payer and card are usually present at the time of the transaction. |
| Terminal | A machine for electronically processing credit card payments. Card data may be captured by swiping the card through a designated slot in the terminal or by keying in the card number by hand. Payment information may be transmitted over phone lines or the Internet. |
| Terminal ID | A unique identifier assigned by the processor to each card accepting device, whether it is a card swipe terminal, POS or a connection through an e-Commerce gateway. |

# Policy Description

## Approval to Accept Merchant Cards

Any NU entity that wishes to accept debit or credit card payments through any medium—e-commerce, paper, terminal, or point-of-sale system—must first have a unique merchant identification number. e-Commerce Operations secures merchant IDs, establishes them with the preferred processor and has them associated with one of the University's bank accounts. Generally, only authorized cash collection units may request to become a card processing merchant.

Merchant card transactions may be processed via e-commerce systems, POS systems, imprint machines, or terminals. A Merchant Card Processing Request Form must be submitted to e-Commerce Operations. Depending on the type of processing (e-Commerce or Terminal), requests are reviewed by up to 4 departments. e-Commerce Operations and Treasury Operations review the request for completeness, forwards it to Accounting Services, and additionally, for e-Commerce requests, to NUIT (through Information & System Security Compliance and the Consulting Project Office).

**Approvals are granted based on a number of factors including, but not limited to the following: strength of the business case, estimated transaction volumes, average dollar amount per transaction, and, the solidity of business processes and internal controls around procedures for collecting, recording, and reconciling sales and credits.**

For e-Commerce requests, in addition to the above, a lot of scrutiny is also placed on the **information and data security of the proposed card processing environment, and whether or not cardholder data and other sensitive information will be stored and/or processed either on a NU server or hosted by a PCI DSS compliant third party service.** Besides a completed PCI DSS SAQ (Self-Assessment Questionnaire) for a proposed e-Commerce solution, a SPSA (Service Provider Security Assessment) may also be warranted prior to receiving NUIT approval. For more information regarding the SPSA process, please consult NUIT's Consulting and Project Office Service Provider Security Assessments page at: http://www.it.northwestern.edu/about/departments/itms/cpo/assessment.html.

Card swipe terminals are acquired through e-Commerce Operations.

## Centrally Managed Revenues

Centrally managed revenues, such as gifts, grants and tuition are the responsibility of special central administrative units. No school or department-based application may solicit or record gifts to the University, grants from sponsors, or tuition for credit courses. The evaluation of tuition payment options for units already taking credit cards will be handled separately from this policy.

## Types of Cards Accepted

Visa, MasterCard, American Express, Discover, Diners Club, and JCB are the only types of merchant cards authorized for use at the University. This is in an effort to contain costs to the departments and the University by directing volume to a limited number of card vendors in order to increase our negotiating power for discount rates.

## Establishing Contracts

All contracts for payment processing systems or services must have prior approval from Treasury Operations and the Office of General Counsel. For e-commerce systems, NUIT must also approve security policies and system architecture. This includes agreements for the lease or purchase of software or hardware as well as the outsourcing of any payment system development or management. It is the responsibility of the NU merchant to ensure that applicable vendors are PCI compliant at the time of signing as well as throughout the life of the contract.

In some cases a third party may suggest that payments be processed under that company's Merchant ID rather than one owned by NU. Prior approval for these arrangements must be obtained from Treasury Operations and the Office of General Counsel in order to ensure that the agreement does not violate any existing contracts.

## Cash Control – Merchant Card Transactions

A daily accounting of receipts from sales should be balanced against merchant card transactions via daily batch settlement reports. The actual funds for the merchant card transactions are electronically deposited into the university's bank account automatically and reconciled by Depository Services. All cash handling units are responsible for complying with the Merchant Card Processing Procedures and NU Cash Handling Policy and Procedures and for developing and maintaining detailed, written departmental balancing procedures.

## Compliance with PCI Data Security Standards

PCI DSS applies to all merchant card processing and its related recordkeeping, whether electronic or on paper. It is the responsibility of the NU Merchant to read and understand the requirements of PCI DSS, although e-Commerce Operations may provide additional guidance.

All merchants must participate in the NU PCI Compliance Program. This program includes the timely completion of a PCI self assessment questionnaire (SAQ) at least annually, and depending on the processing environment, quarterly vulnerability scans. For full details of the requirements of the program see the Credit Card Security (PCI-DSS Compliance) link on the e-Commerce website.

## Security of Non-PCI e-Commerce System Components

For e-commerce/online systems, if the payment processing is outsourced (such as to Paypal) and you do not store, process, or transmit card data on University equipment, those components of the system *may* not fall under the scope of PCI DSS; however, even if you confirm that your system components are outside the scope of PCI DSS, you must take precautions to ensure the security of those system components, including using a firewall to control network traffic. NUIT can provide guidance on security best practices.

Because managing an e-commerce system in accordance with PCI DSS can be challenging and the ramifications of non-compliance to the standards can be significant, all merchants are advised to outsource as much of their system as possible to PCI compliant service providers.

## NUIT Hosting and Network Services

NUIT will provide hosting and network services (including firewall administration) only for components that are outside of the scope of PCI DSS. If PCI DSS compliance services are required for University computing assets or network segments, merchants should consider outsourcing the management of those to a PCI approved service provider.

## Review of Web Content

University Relations reserves the right to review Web content at any time.

## Merchant Card Processing Fees

Merchants are responsible for fees and other costs associated with merchant card processing. The school or department business administrator must review e-commerce business cases and technical requirements to assess the budget and administrative impact due to payment processing activities. The associated startup and recurring costs include, but are not limited to

- fees for credit card transactions,
- equipment rental and maintenance,
- hosting services or equipment costs,
- application and database development and maintenance,
- customer support costs,
- resources to implement and maintain merchant equipment,
- accounting support to do reconciliation, and
- audits and reviews related to PCI compliance.

For a list of current fees see the Merchant Card Processing Fees List.

## Penalties for Noncompliance

Merchant card processing privileges may be revoked at any time if the merchant fails to adhere to this policy and its related procedures. This includes failing to pay associated fees, failing to complete the annual self-assessment questionnaire accurately and in the timeframe dictated, failure to pass required vulnerability scans whenever applicable, and failure to attend annual PCI DSS security training.

In the event that a security breach exposes, or is suspected to have exposed sensitive data, the merchant may be responsible for fines, legal fees, notification costs, and concessionary expenses related to the breach. Additionally, the related merchant account may be revoked.

## Responding to a Card-Related Security Breach

In the event that cardholder data may have been accessed by unauthorized persons, please follow the NU Incident Response Protocol at http://www.it.northwestern.edu/policies/incident.html, and notify e-Commerce Operations immediately via email to Ccard@northwestern.edu or by calling 1-5382. Examples of such incidents include the compromise of electronic information systems as well as loss of paper records.

# Appendices

**Forms:**

Merchant Card Processing Request Form

**Instructions and Procedures:**

NU PCI Compliance Program
Merchant Card Processing Procedures

**Reference:**

Merchant Card Processing Fees List

# Related Information

Payment Card Industry Data Security Standard (PCI DSS)
NU Cash Handling Policy and Procedures
NU Incident Response Protocol

## History/Revision Dates

**Origination Date:** July 8, 2008

**Last Amended Date:** July 31, 2012

**Next Review Date:** January, 2013