NYU | Financial Operations and Treasury

Payment Gateway Definitions

Electronic Payments involve multiple parties to ensure the transaction is processed safely and securely. The parties involved in these transactions are:

- **Customer/Cardholder:**
  An authorized user/owner of the credit card and/or bank account.
- **Issuer:**
  The financial institution that the bank account is set up under and/or the issuer of the credit card, e.g., Bank of America, Provident, Capital One, etc.
- **Merchant:**
  An authorized acceptor of the electronic payment.
- **Merchant ID:**
  Accounts required for a merchant to accept credit card commerce. A merchant ID is setup with an acquirer/processor. NYU's acquiring bank is *Bank of America Merchant Services* (BAMS/FirstData). The Merchant ID can also refer to the primary account in Cybersource. The acquirers merchant ID is necessary before Cybersource can create their own for processing transaction through their system.
- **NYU Middleware:**
  The program(s) that routes the transaction to the Payment Gateway and posts the transaction to FAME and follow-on systems.
- **Payment Gateway:**
  The authorized third party who will collect a customer’s payment information and send it to the Acquiring Bank for approval.
- **Acquiring Bank:**
  The bank that will clear and settle the transactions and remit the funds back to the NYU Merchant.

NYU | Financial Operations and Treasury

Payment Gateway Frequently Asked Questions

How can I accept credit cards?

Departments may accept cards based on expected annual volume. Commerce can be either through eCommerce (web) or POS device (terminal). Approval is based on annual volume and need.

With eCommerce a master Merchant ID has already been setup by school. Departments leverage merchant ID through the use of the Payment Gateway (PGW) technology. Department chartfields are setup in Payment Gateway for every new eCommerce form on PGW.

What cards are accepted?

NYU accepts MasterCard, Visa, American Express, and Discover. JCB and Diners Club are also accepted through the Discover Card network.

On the Payment Gateway transaction report, what is the difference between *Approved* transactions and *Confirmed* transactions?

- Approved transactions are those transactions that were processed successfully in CyberSource, but have yet to be batched to/settled by the bank.
- Confirmed transactions are those transactions that were approved and batched to/settled by the bank.

When your payment page is ready to go into production, the Fiscal Administrator should ensure that the middleware web form is set to Production status. Otherwise, transactions sent through the payment page, while appearing to be successfully processed, will not be credited to your account.

What reports available?

The Payment Gateway has several standard reports. All apply to eCommerce but only the Bank Detail and Bank Summary apply to the POS device credit card revenue:

- Bank Detail Report - Transaction detail from bank
- Bank Summary Report - Deposit Detail from JP Morgan Chase
- Additional Data Report
- Additional data collected from departments payment page (actual web page) .
- Form Request Report
- List of PGW WebForms doing eCommerce under departments primary merchant ID.
- Journal Reconciliation Report

- Report of transaction summary by General Ledger Journal ID. Includes transactions that were paid (confirmed or reversed) only.
- Reconciliation Report
- Includes all transaction. Sorted by Transaction date, report user should note that confirmed and reversed transactions have been paid. Includes the General Ledger Journal ID
- Transaction Report
- Report of all transactions, includes the biographical information from payee.

How do we request refunds?

Refund request MUST be submitted to email address epayments.refund@nyu.edu. The following information MUST be included with request:

- First Name and Last name (from Original Transaction)
- Amount (charged in original transaction)
- Charge Date (Charge Date of the original transaction)
- Amount to be refunded (Whole or Partial amount requested in dollars)
- Merchant ID (alpha character in form creation in Payment gateway during setup)

Who reconciles revenue received from eCommerce?

The business owner (department who setup form) is responsible for reconciliation of the revenue earned. The standard payment gateway reports and UDW reports should be used in this endeavor. The merchants (business owners) using the tool must reconcile their revenue.

What is PCI-DSS (Payment Card Industry - Data Security Standards)?

The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. Initially created by aligning Visa's Account Information Security (AIS)/Cardholder Information Security (CISP) programs with MasterCard's Site Data Protection (SDP) program, the standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents.

The updated version, version 1.1, developed by the founding members of the PCI Security Standards Council, became effective with the launch of the PCI Security Standards Council. New version of more stringent standards takes effect in 2015.

How do you comply with the PCI DSS?

It's a matter of following the requirements in the standard, working with your acquiring bank and using the tools offered through the Council. Remember that PCI DSS compliance is an ongoing process, not a one-time event. You'll need to continuously assess your operations, fix any vulnerabilities that are identified, and make the required reports to the acquiring bank and card brands you do business with. University has contracted vendor Trustwave to assist in this endeavor. FO&T-FSM with guidance of University PCI-DSS Compliance Officer will contact each merchant with requirements and request attestations of compliance which require the use of the web tool provided by Trustwave.

What does Payment Card Industry - Data Security Standards (PCI-DSS) compliance mean?

In security terms, it means that your business adheres to the PCI DSS requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. In operational terms, it means that you are playing your role to make sure your customers' payment card data is being kept safe throughout every transaction, and that they – and you – can have confidence that they're protected against the pain and cost of data breaches.

I got an email from Trustwave asking that I complete Security Awareness Education. Why?

Annual Security Awareness Education (SAE) is part of the PCI-DSS standard. Any staff member handling credit card information are required to complete education every year. Treasury Office administers registration with the assistance of merchant lead/fiscal officer.

The SAE training is required of all members who are:

- Merchant managers responsible for area accepting credit cards,
- Staff actually handling credit card information using a POS terminal
- Webmasters creating website. The webmaster need to understand their responsibilities with data they collect on payment forms doing eCommerce.

Merchant managers are defined for PCI purpose as, fiscal officers with oversight, department managers responsible for Web Team setting up eCommece pages, and managers responsible for locations that have a physical device/terminal.