Merchant Card Processing
Best Practices

Background:

The major credit card companies (VISA, MasterCard, Discover, and American Express) have published a uniform set of data security standards that ALL merchants (i.e. ASU Departments) must comply with in connection with the acceptance of payment cards. These standards are called the Payment Card Industry Data Security Standard or PCI DSS, and the Payment Application Data Security Standard or PA-DSS. These standards place additional responsibilities on university departments in connection with the acceptance of payment cards. DePaul University must comply with these security standards in order to continue to accept payment cards.

Non-compliance with these standards puts DePaul University at risk for:
- Large monetary fines assessed to your department and/or DePaul University
- Loss of merchant status for your department
- Possible loss of merchant status for all of DePaul University
- Loss of faith by the community in the DePaul University name

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.

The PA-DSS standards are to assist software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements.

DePaul University adheres to the highest standards for protecting sensitive data. Payment card data is highly sensitive and therefore must meet the security compliance standards established by the payment card industry. Departments should contact the Treasurer’s Office prior to pursuing any services or applications that may involve accepting credit cards as a form of payment.

Services for processing payment cards, whether through Point of Sale (POS) terminals, mail/telephone order or over the Internet, and any specialized programs or services (e.g. shopping carts, electronic check payments) that link through an electronic bank card authorization system (payment gateway) will be contracted on an University wide level through the Treasurer’s Office in conjunction with the Information Security office.

Departments may only use the services of vendors which have been approved by the Treasurer’s Office and Information Security office to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order or internet based.

Approved merchant departments are to adhere to the Payment Card Data Security Standard, federal, bank and card association regulations and university polices. The merchant department’s ability to accept payment cards is conditioned on complying with, and maintaining these standards and policies. If the merchant department fails compliance, they are responsible for correcting any deficiencies immediately as directed by the Treasurer’s
Office and Information Security Office to bring their merchant department into compliance. Failure to comply with PCI DSS or university policies may result in revocation of merchant department’s privilege to accept payment cards. The merchant department is responsible for all costs associated with any security scans or reviews deemed necessary by the Information Security Office or the Payment Card Associations.

A merchant department that plans to receive revenue from external sales or services and provide taxable goods to customers outside of the university should contact the Tax Manager to discuss sales tax requirements.

All university gifts and donations are processed through the Advancement Office and departments should contact them for additional information on gift processing.

No University employee, contractor or agent who obtains access to payment card or other personal payment information in the course of conducting university business may sell, purchase, provide or exchange said information in any form including, but not limited to, imprinted sales slips, copies of imprinted sales slips, mailing lists, tapes or other media obtained by reason of a payment card transaction to any third party other than to the university’s acquiring bank, depository bank, VISA, MasterCard or other payment card company or pursuant to a government request. All requests to provide information to any party outside of the merchant department must be coordinated with the Information Security Officer and the Treasurer’s Office.

**Best Practices:**

Any university department (“Merchant”) accepting payment cards on behalf of DePaul University for goods or services should designate a full time employee within that department who will have primary authority and responsibility for payment card and/or ecommerce transaction processing within that department. This individual will be referred to hereafter as the Merchant Responsible Person or “MRP”. All MRP’s will be responsible for the department complying with the security measures established by the payment card industry and university policies. In addition, the MRP is responsible to ensure any employee who processes transactions takes the Merchant Training and if applicable have the appropriate background check completed before any access is granted to the employee.

Requests to accept payment cards by university departments are made by completing the Merchant Account form and submitting it to the Treasurer’s Office. Merchant departments may not accept payment cards, or authorize or complete settlement transactions for other university departments.
The following best practices can help you maintain compliance with Payment Card Industry Data Security Standards:

To all Merchants:

- Make sure you **never store Sensitive Authentication Data** *(includes the full track contents of the magnetic stripe or chip, card verification codes and values, PINs and PIN blocks)*.
- Take inventory of all the reasons and places you store this data. If the data doesn’t serve a valuable business purpose, consider eliminating it. **If you don’t need it, don’t store it!**

SAQ A Merchants (Hosted Website) who do not store cardholder data in electronic format and do not process or transmit any cardholder data on their systems or premises:

- Confirm that the third party(s) handling storage, processing, and/or transmission of cardholder data is PCI/DSS compliant, [http://usa.visa.com/merchants/risk_management/cisp_service_providers.html](http://usa.visa.com/merchants/risk_management/cisp_service_providers.html)
- If merchant does store cardholder data, such data is only in paper reports or copies of receipts and is not received electronically, this includes email, and e-fax transmission.
- Restrict physical access to cardholder data
  - Physically secure all media including but not limited to computers, removable electronic media (flash drives for example), paper receipts, paper reports, and faxes in a locked area.
  - Strictly control the internal and external distribution of such media. Do not inter-office or regular unsecured courier.
  - Maintain logs to track all media that is moved from a secured area and obtain management approval prior to moving the media.
  - Maintain strict controls over storage and accessibility of media.
  - Destroy all media that is no longer needed so that cardholder data cannot be reconstructed.
- Maintain a policy that addresses information security for all personnel
  - If cardholder data is shared with service providers, then policies and procedures need to be implemented and maintained to manage service providers:
    - List your relationship with one or more third-party agents, or service providers (for example, gateways, web-hosting companies, etc.).
    - Acknowledgement of the service provider’s responsibility to secure cardholder data must be in the written agreement.
    - Due diligence must be done prior to engagement of service providers and an established process must be in place for engaging service providers.
    - A program must be in place to monitor service provider’s PCI DSS compliance status.

SAQ B Merchants who process cardholder data via imprint machines or standalone, dial-out terminals have to additionally comply with the following:

- List Payment Applications in use (swipe terminal. Etc...) with Version Number and last validated date according to PABP/PA-DSS.
- Merchant uses standalone dial-out terminals that are not connected to the internet or other systems.
- Protect stored cardholder data (IE. Data in swipe terminal, paper receipts, etc...)
  - If sensitive authentication data is received and deleted, then there must be processes in place to securely deleted the data and verify the data is unrecoverable.
  - The full contents of any track are not stored under any circumstances even if encrypted.
  - In the normal course of business only the cardholder’s name, the primary account number (PAN) first and last four digits only, expiration date and service code may be retained.
  - The card verification code or value (three-digit or four-digit number printed on front or back of the payment card) is not stored under any circumstances.
• Unprotected PANs are not to be sent via end-user technologies (email, e-fax, etc...).
• Restrict Access to cardholder data by business need to know.
  o Restrict access to system components (swipe terminals) and cardholder data (paper reports, receipts) to those individuals whose jobs require such access by:
    ▪ Access rights for privileged user IDs restricted by job responsibilities
    ▪ Privileges assigned based on job classification and function (role based)

The following best practices can help you minimize costs.

• To avoid chargebacks, act promptly if contacted directly by the cardholder to resolve a dispute. By working directly with the cardholder to resolve disputes regarding the quality of merchandise or services rendered, you can avoid costly fees and processing costs as well as promote goodwill with your customer.
• If the cardholder does not contact you, respond to inquiries from Merchant Services with as much information as possible about the sales transaction in question.
• Limit one authorization for each settled transaction. Avoid duplicate processing of a transaction and follow the proper procedures for settling your daily transactions.
• Obtain an authorization code. Refuse to process a transaction when you receive a declined code during authorization. Don’t force the settlement of any transactions without a valid authorization.
• To verify cardholder account status, perform a zero value account verification transaction instead of $1.00 authorization transaction.
• Include a description of the goods or services on the transaction receipt.
• Deliver merchandise or services before charging the card.
• Include the CVV2/CVC2 and AVS codes for card not present transactions, if applicable.
• Submit transaction receipts on the same day the transactions are authorized.
• Make sure an imprint appears on a manual transaction receipt or that the relevant transaction information appears on the terminal-generated transaction receipt.
• Do not accept expired cards or cards having effective dates after the date of the transaction.
• Void authorizations within your outstanding batches if they are not going to be settled.
• Call for Voice Authorization, if needed. Call for a Code 10 authorization if you are still suspicious of the cardholder, card, or transaction after receiving an approval code.

Other tips for Reducing Fees:

• Swipe customer cards whenever possible - Swiped cards clear at lower rates than manually-keyed transactions.
• Beware of voice authorization costs - Voice authorizations do not capture the information necessary for lower interchange rates and can generate downgrades.

• Send settlements on time - For transactions where the card is present, settling in two days versus one day can cost you money. If the settlement time extends past two days, this can cost you even more.
• Avoid authorization and settlement amount mismatches - Variations between authorization and settlement amounts are another common cause of downgrades. There are specific industries where
limited tolerance for variations between authorization and settlement amounts are permitted, such as businesses where tipping is commonplace or at hotels or car rental establishments when authorization occurs before the customer’s final invoice is paid

- Distinguish card-not-present (CNP) transactions from hand-keyed transactions where the card is present – Card-Not-Present (CNP) transactions that appear to come from card present channels may be subject to interchange downgrades. In certain types of sales, the card is not physically present for payment. Internet sales and mail or phone orders are the primary examples. CNP transactions carry higher interchange rates because of the inherent risk of fraud. To qualify for more favorable CNP rates, you should make sure that these transactions are easily distinguishable from hand-keyed transactions where the card is present. Usually the best way to do this is to keep these payment operations separate and to use a specific account configuration for each one.

- Ensure your business phone number and a unique order number are passed to us, your card processor, for each transaction - If your customer has easy access to your phone number and the order number on their bill, they may contact you directly rather than disputing a transaction, which may help you avoid costly chargeback fees.

- Capture additional security information - To reduce card fraud in CNP transactions, the Card Associations encourage merchants to capture additional security information in order to qualify for the best interchange rates. To qualify for the lower interchange rate, you need to submit the cardholder’s billing address and zip code for CNP transactions. Capturing this information and passing it via the Address Verification Service (AVS) is an important way for you to control the cost of accepting payments over the phone or on the Internet.

- Capture Levels II and III data when accepting commercial cards - Business, commercial, and purchasing cards are used just like personal credit and debit cards. However, these cards carry higher interchange rates because they offer employers high value (and costly) features such as enhanced reporting and statements. Many merchants can qualify for lower commercial rates (especially in card not present environments) by collecting the more in depth Level II and Level III data with each commercial card transaction. Capturing this information requires greater effort and some cost. It’s wise to verify that your sales volume from commercial cards justifies collecting this data. For more information see the Interchange Qualification Guide
Common sense is the best guide for spotting suspicious behavior. Be sure you combine watchfulness with proper card identification and validation techniques. Be aware of customers who:

- Make indiscriminate large dollar purchases without regard to size, color, style, or price
- Question the sales clerk about credit limits or the authorization process
- Attempt to distract the sales clerk (e.g., continually delay selections, talk continuously)
- Hurry a clerk at quitting time
- Purchase a high-ticket item and insist on taking it immediately, rather than having it delivered—even when delivery is included in the price
- Buy a high-ticket item and request that it be sent next day air or request for someone else to pick up the purchase at a later time
- Pull a card from a pocket rather than a wallet
- Sign the transaction receipt in a deliberate or unnatural manner
- Appear too young to make purchases with a card
- Buy clothing without trying it on for size or decline alterations that are included in the price
- Charge expensive items on a newly valid card
- Do not have a driver’s license, tell you that his or her driver’s license is in the car, or provide only a temporary license without a photo
- Do not ask questions on major purchases
- Make purchases, leave the office, and return to make more purchases
- Make purchases just after the office opens or just before it closes
- Use a card belonging to a friend or relative
- Ship purchases to an address outside of the U.S.
- Recite the card number from memory rather than presenting the card itself
- Ask to see the card again before signing the transaction receipt
RESOURCES

   - Payment Card Processing
   - Records Management
   - Information Security Policy
   - Access to Responsible Use of Data
   - Cash Receipts and Departmental Deposits
   - Fundraising Events and Activities
   - Gift Acceptance and Processing

2. Payment Card Merchant Security Requirements:
   - Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA DSS) https://www.pcisecuritystandards.org/merchants/
   - http://pci.elavon.com
   - Visa USA Cardholder Information Security Program (CISP) http://usa.visa.com/merchants/risk_management/cisp.html
   - MasterCard Worldwide http://www.mastercard.com/sdp
   - American Express: www.americanexpress.com/datasecurity
   - Discover Financial Services: http://www.discovernetwork.com/disc.html

3. Other Requirements:
   - Downtime Procedure - (attached PDF)
   - Business Concept Approval (Academic Affairs Only)-attach PDF
   - http://www.newmerchantassist.com/