

DEFINITIONS DOCUMENT

Cardholder Data	Any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, or any information stored on the magnetic stripe.
Cardholder Dispute	A cardholder can dispute a charge on their credit or debit card for suspecting fraudulent charges, poor service, damaged goods, etc. The merchant is sent a request for the documentation associated with the transaction. Merchant must respond within the given timeframe or a chargeback will occur and the sale will be reversed from the merchant's checking account.
Chargeback	A Credit Card payment that is reversed or taken back from the merchant for various reasons, the most prevalent being an unresolved Cardholder Dispute.
Credit Card	Payment method that allows a consumer to make payments using a line of credit. The authorization and/or charge is applied to a balance that can be paid back over time. Credit Payment Cards are Signature Authorized cards. However, a pin number can be used at an ATM for withdrawing cash from the line of credit. An authorization guarantees payment.
CVV2 Code or CVC Code (CSC, CID, CAV2)	The three digit code on the back of the credit or debit card used as a security feature to guard against fraud. The code is assigned to the card number at random so that hackers are unable to identify that individual code. Used when the magnetic stripe of the card will not read, or for mail, internet, or phone orders. Under no circumstances will Purdue merchants ask for the CVC code.
DBA	Doing Business As: Can be a different name from the corporate entity yet function within the corp. or department.
Debit Card	Payment method that allows a consumer to make payments for goods or services through direct withdrawal from the cardholder's checking account. Debit cards are branded by Visa and MasterCard and can be Signature OR PIN Authorized. The consumer can also receive cash back from participating locations. An authorization guarantees payment.
eCheck	A method of accepting payment by electronically debiting a checking or savings account via the internet.

E-commerce	The ability to process payment cards through a merchant account, eChecks, or other similar payment methods, via the internet as payment for goods or services rendered by the department, utilizing computer software and/or a third party payment application.
Electronic Equipment	Payment card terminals, point of sale registers, kiosks, or where payment card software resides.
Firewall	Hardware, software, or both that protect resources of one network from intruders from other networks. Firewalls must be in place with all Third Party Payment Applications and POS Terminals using an internet/IP connection.
Gateway	A third party software, or the University's U Market software that provides a "shopping card" for your website, so that consumers may enter their card information on a secure site for processing. The Gateway is attached to the payment application for the actual processing.
IP	Internet Protocol
IP Address	Unique numeric code that identifies a particular computer (server) on the Internet.
Merchant Account	An account set up through the bank, which provides the ability to process payment cards, through a card processing company, as payment for goods or services rendered by the account holder via electronic equipment, or E-commerce.
Payment Application	A computer software that utilizes the internet for merchants to process credit and debit cards as payments for goods or services. The application can be a product of a third party processing company, or the UPay application (preferred).
Payment Card	Credit cards, debit cards, or charge cards issued by a financial institution.
Payment Card Acceptance	Processing payment cards through a Point of Sale machine or E-commerce program, as a method of payment for services rendered.

PA DSS	Payment Application Data Security Standards (PA DSS) have been established to guide software vendors and others to develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data. This helps to ensure that their payment applications support compliance with PCI DSS. Any payment application that is sold, distributed or licensed to third parties is subject to the PA DSS requirements. In-house payment applications that are not sold to a third party are not subject to the PA DSS requirements, but must still be secured in accordance with the PCI DSS.
PCI DSS	A world wide security standard developed by Visa Inc International, MasterCard Worldwide, American Express, Discover Financial Services, and JCB International, to protect card holder information and the merchants and/or processors who store that sensitive information from fraudulent use.
PIN	Personal Identification Number. Usually consists of four digits.
POS	Point of Sale. Refers to a face to face transaction with the card present that is processed through a terminal or a register system.
Primary Account Number (PAN)	A 13 to 16 digit credit card or debit card account number that identifies the card issuing bank as well as the individual account holder.
Third Party Processor	A company that offers Payment Card processing software and/or gateway services. All Third Party Processors must be PCI DSS Compliant in order for a department to obtain OR maintain a merchant account.
Truncation	Removing portions of sensitive data. For example: Payment Card numbers may only display the last four digits of the card number. *****1234