

## Card and Payment Account Acceptance and Processing

- Authority** Approved by the Vice President for Business Affairs & Chief Financial Officer.
- Applicability** Applies to all Stanford entities that accept payments via credit or debit card accounts or financial account numbers or third party account numbers. Section 5 of this policy applies to all third-party vendors or service providers that conduct business at Stanford.
- Summary** This policy provides guidelines on acceptance and processing of credit and debit card, account number, or third party account numbers at Stanford.

Section headings:

1. DEFINITION
2. PURPOSE
3. POLICY
4. IMPLEMENTATION GUIDELINES
5. THIRD PARTY VENDORS/SERVICE PROVIDERS OPERATING ON STANFORD'S CAMPUS
6. SOURCES OF MORE INFORMATION

### 1. DEFINITION

The term “card or payment account” as used in this policy includes the use of credit or debit card accounts or account numbers (such as a bank account) or third party account numbers (such as a PayPal or Google accounts). For purposes of this policy, card or payment account acceptance and processing is defined as using any application or device for accepting a card or payment account as payment for goods or services sold by a Stanford University entity. This policy does not apply to Cardinal Dollars or to the University's PCard or Travel credit card programs.

### 2. PURPOSE

A card or payment account provides a convenient way to handle business transactions such as conference registration, the purchase of course materials, or the purchase of meals at a campus dining facility. In order to accept card or payment account payments it is the University's best interest that the acceptance and processing is compliant with Payment Card Industry Data Security Standards for safeguarding card numbers, account numbers, and other prohibited or restricted data as listed in AGM 63. In addition, funds from payments must be securely transferred to the University's financial systems. This policy is to establish guidelines for card or payment account acceptance and processing.

### 3. POLICY

- a. **Relation to University Mission** – Any use of card or payment account acceptance and processing methods at Stanford must be consistent with Administrative Guide Memo 15.3, Unrelated Business Activity, which prohibits the use of Stanford resources for any activity not related to the University's mission.
- b. **Authorized Vendors and Service Providers** – Departments must use a Stanford authorized payment application, payment mechanism, point of sale terminal hardware vendor (if applicable), and a service provider that is listed Visa's Global Registry of Service Providers. These are listed at <http://treasurer.stanford.edu/merchants/>.
- c. **University Merchant Agreement** – Departments wishing to engage in accepting card or payment accounts for the sale of goods or services must be approved by the Treasurer's Office Merchants and Payment Solutions and comply with all terms of the University's Merchant Agreement.

- d. **Information Security** – Card and payment account numbers are classified as Prohibited Data. Departments must comply with [Administrative Guide Memo 63](#), Information Security, and safeguard the confidentiality of Prohibited Data related to purchases of goods or services. They may not store any Prohibited card or payment account information and are required to use secure and encrypted connections to transmit payment information.
- e. **For departments operating electronic commerce web sites:**
  - (1) Departments must post a privacy policy on their web site that is approved by the University Privacy Officer or the Office of the General Counsel. Vendors and/or Service Providers who independently collect card or third party account information must have privacy and terms of use policies on their web sites. These policies must conform to applicable federal and state laws, as well as the University's privacy policies.
  - (2) Third-party advertising is not allowed on any web pages which are hosted on the stanford.edu domain, or which use Stanford's name or emblems. Exceptions to this policy may be granted by the Vice President for Business Affairs and CFO. Advertising does not include mentioning the name of third parties that are co-sponsoring events with Stanford.

#### 4. IMPLEMENTATION GUIDELINES

- a. Merchants accepting card or payment accounts are responsible for complying with Payment Card Industry Data Security Standards (PCI-DSS) and all card brand rules and regulations if applicable, or using secure standard financial industry practices, if PCI DSS standards are not applicable.
- b. Information about requesting a merchant account for payment acceptance is available at the Merchant Services and Payment Solutions website, <http://treasurer.stanford.edu/merchants/>. Departments must work with representatives from the Treasurer's Office (Merchant Services and Payment Solutions), and the Procurement Office to establish and manage card and payment account acceptance and processing.

#### 5. THIRD PARTY VENDORS AND SERVICE PROVIDERS OPERATING ON STANFORD'S CAMPUS

Third party vendors and service providers operating on Stanford's campus must handle data and other information generated from financial transactions involving the Stanford community ("Data") according to Payment Card Industry Security Standards (PCI DSS) Compliance standards at [https://www.pcisecuritystandards.org/security\\_standards/index.php?id=pci\\_dss\\_v1-2.pdf](https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf) (if applicable) or using secure standard financial industry practices, if PCI DSS standards are not applicable.

Stanford reserves the right at any time to request either proof of PCI DSS compliance or a certification (from a recognized third-party security auditing firm) verifying Vendor/Service Provider uses secure standard financial industry practices in its financial transactions, and maintains ongoing compliance under PCI DSS standards and/or employs secure financial industry practices as they change over time.

Vendors and Service Providers must comply with all laws relating to the collection, use, transmission, storage, protection and breach of Data, including but not limited to the California Money Transmission Act. Vendor/Service Provider may not use any Stanford system in connection with financial transactions, and must not store or transmit Data using Stanford's system. Vendor/Service Provider will give immediate notice to the University of any actual or suspected unauthorized disclosure of, access to or other breach of the Data. Vendor/Service Provider is entirely responsible for Data.

## 6. SOURCES OF MORE INFORMATION

- Administrative Guide Memo 14, Academic and Business Relationships with Third Parties - <http://adminguide.stanford.edu/14.pdf>
- Administrative Guide Memo 15.3, Unrelated Business Activity - [http://adminguide.stanford.edu/15\\_3.pdf](http://adminguide.stanford.edu/15_3.pdf)
- Administrative Guide Memo 63, Information Security - <http://adminguide.stanford.edu/63.pdf>
- Stanford authorized payment applications and service providers - <http://treasurer.stanford.edu/merchants/>
- Payment Card Industry Data Security Standards - <http://www.pcisecuritystandards.org>
- Information Security Office - <http://security.stanford.edu>
- Additional information security guidelines, procedures, standards, and practices can be found at <http://securecomputing.stanford.edu>