# PCI Compliance Frequently Asked Questions

**What is the Payment Card Industry (PCI)?**
The Payment Card Industry (PCI) Security Standards Council (SSC) is an open global forum launched in 2006 that is made up of the major payment card associations (MasterCard, Visa, American Express, Discover, and JCB – Japan Credit Bureau) and is responsible for the development, management, education, and awareness of the PCI security standards.

The Payment Card Industry Data Security Standards (PCI DSS) are a set of requirements designed to protect payment card data and cardholder information, and to uphold a secure environment for data management. All UAB PCI Entities (merchants) are required to adhere to these standards.

**Who does PCI affect?**
PCI Security Standards Council requirements must be met by all UAB PCI Entities (merchants) that process, store, transmit, or handle payment card information in any form, in order to protect cardholder data.

**Where can I find the PCI Data Security Standards (DSS)?**
The PCI DSS can be found on the PCI SSC's website at:
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

**What are the penalties for non-compliance with the Payment Card Industry Data Security Standards (PCI DDS)?**
Failure to comply with the PCI security standards may result in disciplinary action which can include suspension or loss of payment card processing capability, monetary fines, or termination of employment. In addition, the payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The bank may pass this fine down to the PCI Entity (merchant), and/or terminate your relationship with the bank or increase transaction fees.

**How do I gain approval to become a UAB PCI Entity?**
The UAB Office of the Chief Financial Officer (CFO) (under the Office of the Vice President of Financial Affairs & Administration) is the UAB focal point for handling the PCI Entity approval and registration process. In order to be granted payment card processing authorization, UAB PCI Entities must complete the approval and registration process with the CFO office, which includes:

- Requesting and completing the PCI Entity Payment Card Account Request Form (A template of this form is also included in Appendix A of the PCI Entity Handbook)
- Obtaining approval signatures on the request form by the Department Head and the Dean or Associate Vice President
- Having all Entity members complete PCI Security Awareness Training and acknowledge the PCI Entity Account Agreement (A template of this form is also included in Appendix C of the PCI Entity Handbook)
- Ensuring all Entity members have had applicable background checks completed (for all new hires and transfers)
- Submitting your Entity business process and procedures for maintaining a secure payment card processing environment to the CFO office.
- Passing an evaluation of internal systems and processes by the CFO office and Information Security, and
- Achieving certification of compliance.

**What are the requirements for achieving certification of compliance?**
In addition to meeting the UAB requirements for PCI Entity approval and registration, the PCI Security Standards Council requires PCI Entities to achieve certification of compliance prior to being authorized to accept payments cards, which includes:

- Documenting compliance by completing a Self-Assessment Questionnaire (guidelines for determining the SAQ appropriate for your Entity are listed in the PCI Entity Handbook), and the CFO's office provides guidance as well.
- Completing the Attestation of Compliance (AOC) as part of the SAQ
- Successfully passing monthly vulnerability scans (where applicable), and
- Submitting the completed SAQ and AOC, evidence of a passing scan, and any other requested documentation to the CFO office.

**How do I know which Self-Assessment Questionnaire (SAQ) my Entity should complete?**
The following guidelines can be used to determine which SAQ is appropriate for your Entity. For additional guidance on which SAQ is appropriate for your Entity, see Appendix D – Self Assessment Questionnaire Selection in the PCI Entity Handbook, the CFO office will also provide guidance.

- SAQ A – Card-not-present merchants; all cardholder data functions are outsourced.
- SAQ B – Imprint-only or stand-alone dial-up terminal merchants with no electronic cardholder data storage.
- SAQ C – Merchants with payment application systems connected to the Internet with no electronic cardholder data storage.
- SAQ D – All other merchants not included in descriptions of SAQ A, B or C above.

**How do I know if my Entity requires monthly vulnerability scans?**
If you electronically store cardholder data post authorization or if your processing systems have any Internet connectivity, a vulnerability scan by a PCI Approved Scanning Vendor (ASV) is required. Only SAQ C and SAQ D Entities require monthly vulnerability scans.

**How do members of my Entity participate in PCI Security Awareness Training?**
Entity management and members can access PCI security awareness training UAB Campus Learning web site at uab.edu/lms. This training offers guidance on local and University-wide payment card policies and procedures regarding the proper handling of cardholder data, and on PCI compliance. Upon accessing the site, you will be required to log in using your Blazer ID and strong password. All PCI Entity members should be pre-registered to take PCI security awareness training. If you are unable to access this training, please contact the CFO office to be registered.

**Once my Entity has been approved, how do I acquire a UAB payment card account?**
Once a UAB PCI Entity has completed the PCI Entity Payment Card Account Request Form, has been approved and registered with the CFO office, and has achieved certification of compliance, the CFO office will provide the requesting Entity with a merchant account and authorization to start processing payment cards.

**My Entity has already been granted payment card processing authorization. Are we required to comply with the new standards?**
Yes. All UAB PCI Entities must be in compliance with new UAB requirements and PCI standards. UAB requirements for PCI Entities are outlined in the PCI Entity Handbook. The current version of the PCI Data Security Standards is version 3.2.1.  UAB PCI Entities will be notified by the CFO office in the event a new version of the PCI DSS is issued.

**What are the requirements for annual re-certification of a UAB PCI Entity?**
Given a UAB PCI Entity's approval and registration date granting authorization to start processing payment cards, those Entities are required to complete the following compliance requirements by that date annually:

- Complete the appropriate Self-Assessment Questionnaire (SAQ) and Attestation of Compliance (AOC)
- Have all Entity management and members complete PCI Security Awareness Training and acknowledge the PCI Entity Account Agreement
- Review Entity scan parameters by those Entities who require monthly vulnerability scans (SAQ C and SAQ D Entities)
- Successfully pass monthly network vulnerability scans performed remotely by a PCI Approved Scanning Vendor (SecureTrust)
- Successfully pass an annual network penetration test performed internally or externally by an approved tester
- Submit all completed PCI documents and forms to the CFO office. (The CFO office provides the PCI forms and documentation to the Entity the month of PCI compliance renewal for the Entity.)

**What initial and/or recurring costs may be the responsibility of my department/unit for processing payment cards?**
Initial and/or recurring costs associated with establishing payment card processing capability and meeting PCI compliance are dependent on the PCI Entity card processing environment. For those Entities that qualify for meeting the compliance requirements of SAQ-A, costs may be minimal and will increase respectively, as the compliance requirements increase for those Entities that qualify for meeting compliance requirements of SAQs B through D. Costs associated with establishing payment card processing capability and with meeting PCI compliance requirements may include, but are not limited to:

- Merchant fees assessed by the credit card companies or the bank
- Obtaining necessary swipe terminal equipment from the bank or acquirer
- Network penetration tests, or follow up re-testing
- Purchasing services from a service provider
- Installing communication lines
- Setting up TouchNet Marketplace services with UAB IT
- Purchasing and/or employing adequate information system security equipment and IT staff
- Responding to breaches or incidents

**What service provider should my Entity use?**
All UAB PCI Entities are encouraged to use the PCI approved service provider, TouchNet Marketplace. Any service provider used by UAB PCI Entities must be compliant with the PCI DSS in order to gain payment card processing authorization from the CFO's office. UAB PCI Entities must contractually obligate their service providers to annually provide documentation that verifies they are certified in complying with the PCI DSS.

**Does UAB have a Privacy Statement that addresses the storage, handling, and processing of payment card data?**
Yes. UAB's payment Card Processing and Security Policy may be accessed at https://www.uab.edu/policies/content/Pages/ .

**Who should I contact if I have questions about PCI requirements?**

- Office of the Chief Financial Officer at 974-5121
- Office of Information Technology (IT) and the AskIT Help Desk at 996-5555.
- UAB IT Information Security Office at 975-0842
- Health System Information Security Help Desk at 934-8888.