Self-Assessment Questionnaire A and Attestation of Compliance
Version 3.2
Guidance Document

The intent of this guidance document is to assist Payment Card Managers in completing their annual PCI DSS Self-Assessment Questionnaire (SAQ) and Attestation of Compliance. Specifically, this document is for use with accounts that qualify to complete an SAQ A (see description below). It should be noted that Payment Card Managers are fully responsible for understanding each question in the SAQ and knowing that their response is accurate within the context of their account(s). The examples provided in this guidance document are for illustrative purposes only.

SAQ A Description: The SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder data. SAQ A merchants are e-commerce merchants (card-not-present), and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

SAQ A merchants confirm that, for this payment channel:

- You accept only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
- You do not electronically store, process, or transmit any cardholder data on your systems or premises, but rely entirely on a third party(s) to handle all these functions;
- You have confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
- You retain only paper reports or receipts with cardholder data, and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s) delivered to your consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

Note: If your merchant account utilizes Authorize.net as a payment gateway, and your integration method is not a Server Integration Method (SIM) or Accept Hosted Integration, contact the Payment Card Program at pmtcard@umn.edu as you may need to complete a different SAQ (SAQ A-EP or SAQ D).

All merchants must comply with the twelve requirements of the Payment Card Industry Data Security Standards (PCI DSS). However, the self-assessment for SAQ A merchants focuses on portions of two standards:

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 8: Identify and authenticate access to system components

Requirement 9: Restrict physical access to cardholder data

Requirement 12: Maintain a policy that addresses information security for all personnel

The following chart offers helpful hints and common findings for completing your PCI DSS SAQ A.

SAQ Questions, Helpful Hints & Common Findings

Section 1: Assessment Information	
SAQ Section or Question	**Helpful Hints & Common Findings**
Merchant and Qualified Security Assessor Information Part 1a. Merchant Organization Information	Complete this section with the contact information for your merchant area/department including the contact information for the merchant manager who has responsibility for the merchant account and the payment card activities in the office. Note: Company Name should be "Regents of the University of Minnesota", and DBA (doing business as) should be your Payment Card Account Name.
Part 1b. Qualified Security Assessor Company Information (if applicable)	Since the University rolls our SAQs up into a single report to submit to our acquiring bank you can leave this section blank.
Executive Summary Part 2a. Type of Merchant Business (check all that apply)	Select the type of business that is applicable to your area or department. Most often, this is limited to "E-Commerce" for SAQ-A merchants. Check the types of credit and debit card payment channels that your area uses. Most often, this is limited to "E-Commerce" for SAQ-A merchants. Check the types of payment channels that are covered by this SAQ. Most often, this is limited to "E-Commerce" for SAQ-A merchants.
Part 2b. Description of Payment Card Business	Describe your payment card environment in detail. Be sure to include an explanation of: 1. *What the customer is purchasing,* 2. *How you process credit card payments (your payment card environment), and* 3. *Any service provider(s) and how they interact with your payment card environment.* An example description may be, "The department has a merchant account which allows us to accept credit and debit card payments for our online supplemental application fee. The customer is directed to the department's online application website, where they complete their application and are automatically redirected to our payment gateway (Authorize.net) for processing of their payment card.

Part 2c. Locations	Describe the type of facility included in your PCI DSS review. Most often, the type of facility for SAQ A merchants is limited to "Office or Departmental Setting" as your process involves e-commerce sales.
Part 2d. Payment Application	Payment Applications are systems or software that are: 1. Hosted and managed by the University, and 2. Used to store, process, or transmit cardholder data electronically. An example of a Payment Application is a Point of Sale system. *Most often, for SAQ A merchants, there are no payment applications being used as you are processing payments through the use of a third-party payment gateway, such as Authorize.net.*
Part 2e. Description of Environment	"Provide a high-level description of the environment covered by this assessment." Most often, a high-level description of an SAQ A environment is limited to a statement such as "For payment card transactions, the department uses a University website redirecting to Authorize.net (a PCI DSS validated third-party payment processor)". "Does your business use network segmentation to affect the scope of your PCI DSS environment?" *For SAQ A merchants, payment card transactions are not transmitted using the University's network, so the answer to this question will be "No".*
Part 2f. Third-Party Service Providers	"Does your company use a Qualified Integrator & Reseller (QIR)?" *For SAQ A merchants, you most likely do not use a Qualified Integrator and Reseller Company (QIR Company) to implement, configure, and/or support your payment card applications, so the answer to this question would be "No".* "Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?"

	A third-party service provider is any company that stores, transmits, or processes payment cards for the University; or any entity that can affect the security of cardholder data. Examples of third-party service providers include Authorize.net, AudienceView, Amazon Web Services, PayPal, RegOnline, and others. Make sure to list all third-party service providers that your area uses to store, transmit, or process payment cards. *Note: Requirement 12.8 applies to all entities in this list.*
Part 2g. Eligibility to Complete AOC SAQ A	Carefully read each of the six statements. Check each statement that is true for your account. If any statements are not true for your account, or if you are unsure, contact the Payment Card Program at pmtcard@umn.edu.
Section 2: Self-Assessment Questionnaire	
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.
2.1 (a) Are vendor-supplied defaults always changed before installing a system on the network? *This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).*	Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password. As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer "Yes" to this question if both of the following are correct: 1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure for vendor-supplied defaults to always be changed.

	2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure for vendor-supplied defaults to always be changed.
2.1 (b) Are unnecessary default accounts removed or disabled before installing a system on the network?	As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer "Yes" to this question if the following is correct: 1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure that unnecessary default accounts are removed or disabled before installing a system on the network. 2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure that unnecessary default accounts are removed or disabled.
Requirement 8: Identify and authenticate access to system components	Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes. The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.
8.1.1 Are all users assigned a unique ID before allowing them to access system components or cardholder data?	As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer "Yes" to this question if the following is correct: 1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure that all users are assigned a unique ID before allowing them to access the server. 2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure that all users are assigned a unique ID before allowing them to access the payment gateway.

8.1.3 Is access for any terminated users immediately deactivated or removed?	As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer "Yes" to this question if the following is correct: 1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure that access to the server for any terminated users is immediately deactivated or removed. 2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure that access to the gateway for any terminated users is immediately deactivated or removed.
8.2 In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? • *Something you know, such as a password or passphrase* • *Something you have, such as a token device or smart card* • *Something you are, such as a biometric*	As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer "Yes" to this question if the following is correct: 1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure to authenticate users with a unique ID, as well as something you know, something you have, or something you are. 2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure to authenticate users with a unique ID, as well as something you know, something you have, or something you are.
8.2.3 (a) Are user password parameters configured to require passwords/passphrases meet the following? • *A minimum password length of at least seven characters* • *Contain both numeric and alphabetic characters* Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. You are able to answer "Yes" to this question if the following is correct: 1. You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure that user's password parameters include a minimum length of seven characters and contain both numeric and alphabetic characters. 2. You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure that user's password parameters include a minimum length of seven characters and contain both numeric and alphabetic characters.

8.5 Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: • *Generic user IDs and accounts are disabled or removed;* • *Shared user IDs for system administration activities and other critical functions do not exist; and* • *Shared and generic user IDs are not used to administer any system components?*	As an SAQ-A merchant, you should be redirecting your customers from a University website to a payment gateway such as Authorize.net. <u>You are able to answer "Yes" to this question if the following is correct:</u> 1. <u>You can confirm that, for the server which hosts the website which redirects to a payment gateway for processing, it is standard procedure to prohibit group, shared, or generic accounts.</u> 2. <u>You can confirm that, for the payment gateway which processes your online credit card payments, it is standard procedure to prohibit group, shared, or generic accounts.</u>
Requirement 9: Restrict physical access to cardholder data	Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data. Two common findings are (1) the need to recognize where increased security is required, and (2) to document all operational procedures in writing.
9.5 Are all media physically secured? *(media includes computers, removable electronic media, hard drives, portable drives, USB sticks, CDs, DVDs, paper reports, paper receipts, and faxes)*	Because SAQ-A merchants do not typically interact with any media containing cardholder data, this item is typically marked "Not Applicable (N/A)". For example, SAQ-A merchants typically do not take phone orders, fax orders, or enter a customer's data at their request. In short, SAQ-A merchants should never see or have access to full card numbers. If this is not the case with your account, you may need to answer this question "NO" and contact the Payment Card Program at pmtcard@umn.edu to develop a remediation plan.
9.6 (a) Is strict control maintained over the internal or external distribution of any kind of media? 9.6 (b) Do controls include the following: 9.6.1 Is media classified so the sensitivity of the data can be determined?	Typically, this is answered as "Not Applicable (N/A)" as SAQ-A merchants do not typically interact with any media containing cardholder data. For example, SAQ-A merchants typically do not take phone orders, fax orders, or enter a customer's data at their request. In short, SAQ-A merchants should never see or have access to full card numbers.

9.6.2 Is media sent by secured courier or other delivery method that can be accurately tracked? 9.6.3 Is management approval obtained prior to moving the media?	If this is not the case with your account, you may need to answer this question "NO" and contact the Payment Card Program at pmtcard@umn.edu to develop a remediation plan.
9.7 Is strict control maintained over the storage and accessibility of media?	Typically, this is answered as "Not Applicable (N/A)" as SAQ-A merchants do not typically interact with any media containing cardholder data. For example, SAQ-A merchants typically do not take phone orders, fax orders, or enter a customer's data at their request. In short, SAQ-A merchants should never see or have access to full card numbers. If this is not the case with your account, you may need to answer this question "NO" and contact the Payment Card Program at pmtcard@umn.edu to develop a remediation plan.
9.8 (a) Is all media destroyed when it is no longer needed for business or legal reasons? 9.8 (c) Is media destruction performed as follows: 9.8.1 (a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed? 9.8.1 (b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	Typically, this is answered as "Not Applicable (N/A)" as SAQ-A merchants do not typically interact with any media containing cardholder data. For example, SAQ-A merchants typically do not take phone orders, fax orders, or enter a customer's data at their request. In short, SAQ-A merchants should never see or have access to full card numbers. If this is not the case with your account, you may need to answer this question "NO" and contact the Payment Card Program at pmtcard@umn.edu to develop a remediation plan.
Requirement 12: Maintain a policy that addresses information security for all personnel	A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment. A common concern in this area is ensuring that merchants maintain adequate payment card procedures which include explanations on employee training and termination, how customers pay for purchases, disposal of cardholder data, and incident response. *Note: Each merchant must have a written statement in their operational procedures stating they comply with University of Minnesota Information Security Policies and Procedures.*

12.8.1 Is a list of service providers maintained? *Note: A third-party service provider is any company that stores, transmits, or processes payment cards for the University, as well as any company that could affect the security of a cardholder transaction.*	As SAQ-A accounts are e-commerce accounts, your process normally involves a third party service provider supplying the payment gateway which processes your online credit card payments. Your process may also involve a third party service provider which hosts the website that redirects to your payment gateway for processing. *Examples of third-party service providers include Authorize.net, AudienceView, Amazon Web Services, and others.* *The answer to this question should be "Yes", as the Accounts Receivable Services department maintains a list of service providers.*
12.8.2 Is a written agreement maintained that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess?	For University-wide third party service providers such as Authorize.net and AudienceView, this agreement is created and maintained through the vendor contract which typically involves Purchasing, OGC, and the Controller's Office. If your account uses a third party service provider, you should have worked with Accounts Receivable Services (ARS) to ensure that an appropriate agreement was established and that a copy of the most recent agreement was provided to ARS. *The answer to this question should be "Yes", as the Accounts Receivable Services department maintains a written agreement with the service provider.* For PCI DSS compliance purposes, the Payment Card Manager must know that this agreement exists and that it can be found in the Accounts Receivable Services department.
12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?	*The answer to this question should be "Yes", as the Accounts Receivable Services department maintains an established process for engaging service providers.* The University's Accounts Receivable Services Department, Purchasing Department, and Office of General Counsel (OGC) all have an established process for engaging service providers that interact with cardholder data on behalf of the University. The Payment Card Manager must be aware that all of these areas have an established process in place for engaging payment card service providers prior to the use of the service provider…and this established process must be utilized whenever new payment card service providers are to be introduced to your environment.

12.8.4 Is a program maintained to monitor service providers' PCI DSS compliance status?	*The answer to this question should be "Yes", as the Accounts Receivable Services department monitors the service providers' PCI DSS compliance via contractual language.*
12.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider?	*The answer to this question should be "Yes", as the Accounts Receivable Services department works with the service provider to ensure that appropriate requirements are managed by all parties.*
12.10.1 (a) Has an incident response plan been created to be implemented in the event of system breach?	If you maintain and annually review the UM1634 Form "Incident Response and Continuity Plan", you can typically answer "Yes" to this question. Keep in mind that this form has to be uploaded to the CampusGuard Document Locker annually as well.
Appendix B: Compensating Controls Worksheet	
Compensating Controls Worksheet	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must: 1) Meet the intent and rigor of the original stated PCI DSS requirement; 2) Provide a similar level of defense as the original PCI DSS requirement; 3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement. **If you answered "Compensating Control Used" to any of the questions shown in the requirement sections, contact pmtcard@umn.edu for further guidance on how to complete this section.** Typically, merchants do not use compensating controls, so this section can be left blank.
Appendix C: Explanation of Non-Applicability	
Explanation of Non-Applicability	If you answered "Not Applicable (N/A)" to any of the questions shown in the requirement sections, you are required to use this worksheet to explain why the related requirement is not applicable to your area.

Section 3: Validation and Attestation Details	
Part 3. PCI DSS Validation	After completing the body of the SAQ, if you answered "Yes" or "Not Applicable (N/A)" to all the questions asked in the requirements sections, your area is compliant and you can check the "Compliant" box. **If you answered "No" to any of the questions asked in the requirements sections, your area is non-compliant, and you need to contact the Payment Card Program at pmtcard@umn.edu for assistance completing this section.** Typically, "Compliant but with Legal Exception" is not checked.
Part 3a. Acknowledgement of Status	After completing the body of the SAQ carefully read each of the statements shown in this section, and check each statement that is true for your account. • *PCI DSS Self-Assessment Questionnaire A, Version 3.20, was completed according to the instructions therein.* • *All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.* • *I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.* *For this SAQ, all payment processing functions are fully outsourced to a third party such as Authorize.net. If you utilize Authorize.net as your payment processor, you can typically check this box as Authorize.net does not store sensitive authentication data after authorization. If your area uses a payment processor other than Authorize.net, you will need to check with that processor to verify that they do not store sensitive authentication data after authorization.* • *I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.* • *If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.*

	• *No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during this assessment.* *If your payment process utilizes the use of Authorize.net, you can typically check this box as Authorize.net does not store full track data, CAV2, CVC2, CID, CVV2 data, or PIN data after authorization.* • *ASV scans are being completed by the PCI SSC Approved Scanning Vendor* *As ASV scans are not required for merchants redirecting to a payment processor for payment, you should be able to leave this question blank.* If you are unsure about any of the questions shown in this section, contact the Payment Card Program at pmtcard@umn.edu.
Part 3b. Merchant Attestation	After completing the body of the SAQ the Payment Card Manager is to type in the current date, and enter their name and title as the "Merchant Executive Officer".
Part 3c. QSA Acknowledgement (if applicable)	**This section does not need to be completed.**
Part 3d. ISA Acknowledgement (if applicable)	**This section does not need to be completed.**
Part 4. Action Plan for Non-Compliant Status	This section is a summary of the PCI DSS requirements shown in your questionnaire. If you answered "Yes" or "Not Applicable (N/A)" to all the questions asked in the requirements sections, your area is compliant and you can check "Yes" for each line item. **If you answered "No" to any of the questions asked in the requirements sections, your area is non-compliant and you need to contact the Payment Card Program at pmtcard@umn.edu for assistance completing this section.**