Self-Assessment Questionnaire B 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 B (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 B Description: The SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals. SAQ B merchants may be either brick-and-mortar (card-present) or mail/telephone order (card-not-present) merchants, and do not store cardholder data on any computer system.

SAQ B merchants confirm that, for this payment channel:

- You use only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information;
- The standalone, dial-out terminals are not connected to any other systems within your environment;
- The standalone, dial-out terminals are not connected to the Internet;
- You do not transmit cardholder data over a network (either an internal network or the Internet);
- You retain only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; and
- You do not store cardholder data in electronic format.

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

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 7: Restrict access to cardholder data by business need to know

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 B.

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 "MOTO" for SAQ-B merchants. If you are completing this SAQ for an e-commerce account as well as a dial-up or cellular terminal, you may want to select "E-Commerce" as well as "MOTO". Check the types of credit and debit card payment channels that your area uses. Most often, this is limited to "MOTO" and/or "Card-present (face-to-face)" for SAQ-B merchants. If you are completing this SAQ for an e-commerce account as well as a dial-up or cellular terminal, you may want to select "E-Commerce" as well as "MOTO" and/or "Card-present (face-to-face). Check the types of payment channels that are covered by this SAQ. Most often, this is limited to "MOTO" and/or "Card-present (face-to-face)" for SAQ-B merchants. If you are completing this SAQ for an e-commerce account as well as a dial-up or cellular terminal, you may want to select "E-Commerce" as well as "MOTO" and/or "Card-present (face-to-face).
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 for two dial-up swipe terminals which allows us to accept credit and debit card payments for the sales of admission fees as well as merchandise. The customer can pay in-person or via phone call.
Part 2c. Locations	Describe the type of facility included in your PCI DSS review. Most often, the type of facility for SAQ B merchants is limited to "Office or Departmental Setting", "Front Desk", or "Cashier Office" as your process involves dial-up of cellular swipe terminals.
Part 2d. Payment Application(s)	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 B merchants, there are no payment applications being used as you are processing payments through the use of a stand-alone payment terminal.*
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 B environment is limited to a statement such as "For payment card transactions, the department uses a standalone dial-up swipe terminal connected via a phone line to Wells Fargo Merchant Services". "Does your business use network segmentation to affect the scope of your PCI DSS environment?" *For SAQ B 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 B merchants, you most likely do not use a Qualified Integrator and Reseller Company (QIR Company) to implement, configure, and/or support your payment card environment, 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, Active Networks, 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 SAQ B	Carefully read each of the four statements. Note the first box includes two statements joined by "and/or". As long as one statement is true for your account you may check the box. 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 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

University of Minnesota SAQ-B accounts typically answer each question in this section "Yes".

However, a common finding by outside assessors is the lack of written procedures that document how a merchant complies with specific PCI DSS requirements, such as Requirement 3. The University maintains written information security policies that apply to merchant accounts. However, each merchant must create and maintain written operational procedures that reference broader University policies and detail day-to-day practices associated with the merchant account. Procedures can be brief and may be incorporated into other written procedures in the unit.

Below are examples of common operational procedures for Requirement 3 questions for SAQ-B accounts. You may add to and customize these to develop the procedures that apply to your practices. Operational procedures are not included with the SAQ, but are used to train unit employees, and must be readily available to share on request. As such, all written documents relating to your merchant account(s) should be placed in the CampusGuard Document Locker provided with your portal account. THESE ARE EXAMPLES. THE PROCEDURES DESCRIBED MAY NOT BE APPLICABLE TO YOUR AREA. THE GOAL IS TO DOCUMENT EACH STEP IN THE ACCEPTANCE OF PAYMENT CARDS FOR YOUR ACCOUNT, AS THOUGH WRITING THEM FOR A NEW EMPLOYEE.

1. Phone payments "When accepting a customer's payment card information over the phone, the merchant manager [or his/her designee] writes the card information on a piece of paper, immediately enters the data into the swipe terminal, and immediately shreds the paper in a cross-cut shredder. If the merchant manager is unable to immediately enter the data and shred the paper, the paper containing cardholder data is placed in a locked cabinet, drawer, or safe to which only the merchant manager and a designee have access."

2. Display of card numbers in accounting system "Only the last 4 digits of card numbers are displayed in systems used to reconcile accounts." [Note: The last 4 digits of card numbers alone do not constitute "cardholder data", and thus the systems storing this data are out of scope for PCI DSS.]

3. What to do if cardholder data is received via email "Cardholder information may not be received through email. In the rare case that a customer emails their cardholder data to the department, delete the email, empty your recycle bin, follow other procedures as recommended by University Information Security, contact the customer immediately via a separate email or by phone to explain that the University may not accept card information via an email for security reasons, and describe their available options."

4. Paper-based remittance forms "Paper-based remittance forms are designed with a tear-off portion for the customer's card data which can be torn off and shredded immediately after processing. Mailed-in invoices are received, opened, and processed by the merchant manager [or his/her designee] the day they are received or as soon as possible. Unprocessed invoices and unopened mail expected to contain customer payment data are kept in a secure area such as a safe or locked file that is only accessible by the merchant manager or a designee."

Requirement 4: Encrypt transmission of cardholder data across open, public networks *Requirement 4.2 (b) Are policies in place that state unprotected PANs are not to be sent via end-user messaging technologies?*	Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments. Although this is covered at a high level by University data security and privacy policies, add a statement to your operational procedures to reflect compliance with this item (see #3 under Requirement 3 above "What to do if cardholder data is received via email").

Requirement 7: Restrict access to cardholder data by business need to know	To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job. You can typically answer "Yes" to this question if you limit access to your swipe terminal(s) and cardholder data (paper forms or the actual card as shared in person by the card holder) to only those individuals whose jobs require access; for example, the Payment Card Manager and cashiers. If your area does not limit access to your swipe terminal(s) and cardholder data to only those individuals with a business need, contact the Payment Card Program at pmtcard@umn.edu to discuss your process. *Note: Reports used for account reconciliation that only list the last 4 digits of a card number do not constitute cardholder data for PCI DSS.*
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. Below are common findings by the outside assessor and examples of written procedures the can be customized to fit your situation.
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)*	Paper documents with cardholder data were sometimes handled with outdated methods, such as not keeping them in locked storage at all times other than when being processed. See example #4 under Requirement 3 above.

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? 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?	An example of written operational procedures that demonstrate compliance are: "Paper remittance forms received in person or via the mail that contain cardholder information are…"[describe the processes followed from receipt of the form to shredding the form] 9.6.1 If paper documents containing cardholder data are stored before processing, they should be separated from other documents and marked appropriately (ex: "confidential"; "highly confidential for immediate processing"). 9.6.2 If paper documents containing cardholder data must be moved from one secure location to another, they should be carried by hand by the Payment Card Manager or designee. 9.6.3 If paper documents containing cardholder data must be moved from one secure location to another, approval from the Payment Card Manager is required prior to moving the cardholder data.
9.7 Is strict control maintained over the storage and accessibility of media?	For example, are paper documents containing cardholder data accessible to only those with a job need? Are all hardcopy cardholder data kept in a locked drawer, file or safe if not processed immediately upon receipt?
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?	In this context, the destruction of media refers to cross-cut shredding any paper with cardholder data immediately after processing. *The University does not recommend using storage containers for the disposal of cardholder data after processing.*
9.9 Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows? 9.9 (a) Do policies and procedures require that a list of such devices maintained? 9.9 (b) Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	9.9 (a) Completing and uploading your Payment Card Inventory List to the CampusGuard Document Locker would typically address this question. 9.9 (b) and 9.9 (c) Your procedures should include inspecting your swipe terminal for tampering and substitution upon use, and reporting any suspicious behavior or possible tampering to abuse@umn.edu.

9.9 (c) Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	
9.9.1 (a) Does the list of devices include the following? Make, model of device Location of device Device serial number 9.9.1 (b) Is the list accurate and up to date? 9.9.1 (c) Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	Maintaining a Payment Card Inventory List and reviewing and uploading this list to the CampusGuard Document Locker annually would typically address these questions.
9.9.2 (a) Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows? 9.9.2 (b) Are personnel aware of procedures for inspecting devices?	Ensuring that your procedures include inspecting your swipe terminal upon use, and reporting possible tampering (unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings), would typically address these questions. All employees responsible for processing payment card transactions using your payment card terminal(s) should also be aware of this requirement.
9.9.3 Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following? 9.9.3 (a) Do training materials for personnel at point-of-sale locations include the following? • Verify the identity of any third party persons claiming to be repair or maintenance personnel. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices. • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel. 9.9.3 (b) Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?	Ensuring that your procedures include inspecting your swipe terminal upon use, and reporting possible tampering (unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings), would typically address these questions.

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.*
12.1 Is a security policy established, published, maintained, and disseminated to all relevant personnel?	If you maintain and annually review a "Department Payment Card Operational Procedures" document you are able to answer "Yes" to this question. Keep in mind that this "Payment Card Operational Procedures" document has to be uploaded to the CampusGuard Document Locker annually as well.
12.1.1 Is the security policy reviewed at least annually and updated when the environment changes?	If you maintain and annually review a "Department Payment Card Operational Procedures" document can typically answer "Yes" to this question. Keep in mind that this "Payment Card Operational Procedures" document has to be uploaded to the CampusGuard Document Locker annually as well.
12.3 Are usage policies for critical technologies developed to define proper use of these technologies and require the following: *Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* 12.3.1 Explicit approval by authorized parties to use the technologies?	The University maintains authorization approval policies for critical technologies. If you maintain language in your Payment Card Operational Procedures talking about who has authorization to use your critical technologies (ex. swipe terminal is only to be used by the Payment Card Manager and employees who have been appropriately trained and signed a UM1623 form, etc.), you can typically answer "Yes" to this question.

12.3.3 A list of all such devices and personnel with access?	The University maintains a list of all critical devices and those authorized to access these devices. If you maintain a "Payment Card Inventory List" and ensure that employees with access to your critical technologies are trained and documented, you can typically answer "Yes" to this question.
12.3.5 Acceptable uses of the technologies?	The University maintains authorization approval policies for critical technologies. If you maintain language in your Payment Card Operational Procedures talking about the acceptable uses of any critical technologies (ex. wireless access not allowed for payment processing, employees not allowed to process payments using their work computer, etc.), you can typically answer "Yes" to this question.
12.4 Do security policy and procedures clearly define information security responsibilities for all personnel?	The University maintains security policies and procedures which define security responsibilities for all personnel. If you maintain language in your Payment Card Operating Procedures talking about the importance of payment card security as well as who is responsible for ensuring this security, you can typically answer "Yes" to this question.
12.5 (b) Are the following information security management responsibilities formally assigned to an individual or team: 12.5.3 Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	The University maintains a security incident response team to ensure timely and effective handling of all situations. If you maintain and annually review the UM1634 Form "Incident Response and Continuity Plan", you can typically answer "Yes" to this question.
12.6 (a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?	The University maintains a formal security awareness program. If you have completed all assigned training videos and training workshops and have instituted and maintain a payment card training program for your employees, you can typically answer "Yes" to this question.
12.8 Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows: 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*	Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked "Not Applicable (N/A)" (with a corresponding statement such as "Data is not shared with service providers" in Appendix C: Explanation of Non-Applicability.

cardholder transaction. Examples of third-party service providers include Authorize.net, AudienceView, Amazon Web Services, and others.	
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?	Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked "Not Applicable (N/A)" (with a corresponding statement such as "Data is not shared with service providers" in Appendix C: Explanation of Non-Applicability.
12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?	Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked "Not Applicable (N/A)" (with a corresponding statement such as "Data is not shared with service providers" in Appendix C: Explanation of Non-Applicability.
12.8.4 Is a program maintained to monitor service providers' PCI DSS compliance status?	Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked "Not Applicable (N/A)" (with a corresponding statement such as "Data is not shared with service providers" in Appendix C: Explanation of Non-Applicability.
12.8.5 Is information maintained about which PCI DSS requirements are managed by each service provider?	Typically, SAQ-B accounts do not involve third party service providers. If this is the case in your instance, each question in Requirement 12.8 may be marked "Not Applicable (N/A)" (with a corresponding statement such as "Data is not shared with service providers" in Appendix C: Explanation of Non-Applicability.
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 B, 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.* *The typical payment system for this SAQ is a dial-up or cellular swipe terminal. Dial-up and cellular swipe terminals 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.* *The typical payment system for this SAQ is a dial-up or cellular swipe terminal. Dial-up and cellular swipe terminals do 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 dial-up or cellular payment terminals 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.**