PCI DSS Question		Response		
		Yes	No	N/A
12.2.a	Is an annual risk assessment process implemented that: * Identifies critical assets, threats, and vulnerabilities, and * Results in a formal, documented analysis of risk? Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.	☑	☐	
12.2.b	Is the risk assessment process performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)?	☑	☐	
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?	☑	☐	
12.3.2	Authentication for use of the technology?	☑	☐	
12.3.3	A list of all such devices and personnel with access?	☑	☐	
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)?	☑	☐	
12.3.5	Acceptable uses of the technologies?	☑	☐	
12.3.6	Acceptable network locations for the technologies?	☑	☐	
12.3.7	List of company-approved products?	☑	☐	
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?	☑	☐	
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?	☑	☐	

	PCI DSS Question	Response		
		Yes	No	N/A
12.3.10.a	For personnel accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need? Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	☑	☐	
12.3.10.b	For personnel with proper authorization, does the policy require the protection of cardholder data in accordance with PCI DSS Requirements?	☑	☐	
12.4	Do security policy and procedures clearly define information security responsibilities for all personnel?	☑	☐	
12.5.a	Is responsibility for information security formally assigned to a Chief Security Officer or other security-knowledgeable member of management?	☑	☐	
12.5.b	Are the following information security management responsibilities formally assigned to an individual or team:			
12.5.1	Establishing, documenting, and distributing security policies and procedures?	☑	☐	
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?	☑	☐	
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	☑	☐	
12.5.4	Administering user accounts, including additions, deletions, and modifications?	☑	☐	
12.5.5	Monitoring and controlling all access to data?	☑	☐	
12.6.a	Is a formal security awareness program in place to make all personnel aware of the cardholder data security policy and procedures?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
12.6.b	Do security awareness program procedures include the following:			
12.6.1.a	Does the security awareness program provide multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions)? Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	☑	☐	
12.6.1.b	Are personnel educated upon hire and at least annually?	☑	☐	
12.6.1.c	Have employees completed awareness training and are they aware of the importance of cardholder data security?	☑	☐	
12.6.2	Are personnel required to acknowledge at least annually that they have read and understood the security policy and procedures?	☑	☐	
12.7	Are potential personnel (see definition of "personnel" above) screened prior to hire to minimize the risk of attacks from internal sources? Examples of background checks include previous employment history, criminal record, credit history and reference checks. Note: For those potential personnel to be hired for certain positions, such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	☑	☐	
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, including a description of the service(s) provided?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	☑	☐	
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	☑	☐	
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	☑	☐	
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	☑	☐	
12.10	Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:			
12.10.1.a	Has an incident response plan been created to be implemented in the event of system breach?	☑	☐	
12.10.1.b	Does the plan address the following, at a minimum:			
12.10.1.b.1	* Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?	☑	☐	
12.10.1.b.2	* Specific incident response procedures?	☑	☐	
12.10.1.b.3	* Business recovery and continuity procedures?	☑	☐	
12.10.1.b.4	* Data backup processes?	☑	☐	
12.10.1.b.5	* Analysis of legal requirements for reporting compromises?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
12.10.1.b.6	* Coverage and responses of all critical system components?	☑	☐	
12.10.1.b.7	* Reference or inclusion of incident response procedures from the payment brands?	☑	☐	
12.10.2	Is the plan reviewed and tested at least annually, including all elements listed in Requirement 12.10.1?	☑	☐	
12.10.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts?	☑	☐	
12.10.4	Is appropriate training provided to staff with security breach response responsibilities?	☑	☐	
12.10.5	Are alerts from security monitoring systems included in the incident response plan?	☑	☐	
12.10.6	Is a process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?	☑	☐	