PCI DSS Requirement	Description	Frequency	Scope
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing a web-application firewall in front of public-facing web applications	Presuming no Web Application Firewall in place, at least annually, or after any changes	External or Internal
11.1	Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*	At least quarterly, *irrespective of use of wireless devices*	Internal and/or External as appropriate
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3)*	At least quarterly, or after significant change. See 11.2.1, 11.2.2 and 11.2.3 below	Internal & External

PCI DSS Requirement	Description	Frequency	Scope
	vulnerabilities noted in the scan results have been corrected as shown in a rescan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.		
11.2.1	Perform quarterly internal vulnerability scans.	Quarterly	Internal
11.2.2	Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.*	Quarterly	External

PCI DSS Requirement	Description	Frequency	Scope
11.2.3	Perform internal and external scans after any significant change. ***Note:*** *Scans conducted after changes may be performed by internal staff.*	After significant change	Internal and External
11.3	Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a subnetwork added to the environment, or a web server added to the environment). These tests must include both Network-layer penetration tests (11.3.1) and Application-layer penetration tests (11.3.2)	Annually, or after significant change	Internal & External