

Payment Card Industry (PCI) Executive Report

06/08/2017

ASV Scan Report Attestation of Scan Compliance

Scan Status

- * Compliance Status : **PASS**
- * Scan report type: Full scan
- * Number of unique components scanned: 1
- * Number of identified failing vulnerabilities: 0
- * Number of components found by ASV but not scanned because scan customer confirmed components were out of scope: 18
- * Date scan completed: 06/06/2017
- * Scan expiration date (90 days from date scan completed): 09/04/2017

Scan Customer Attestation

Action Corporation attests on 06/08/2017 at 19:54:13 GMT that this scan includes all components* which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. Action Corporation also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicated whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

ASV Attestation

This scan and report was prepared and conducted by Qualys under certificate number 3728-01-11, according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS ASV Program Guide.

Qualys attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active scan interference. This report and any exceptions were reviewed by Qualys PCI Support

Part 1. Scan Information

Scan Customer Company:	Action Corporation	ASV Company:	Qualys
Date scan was completed:	06/06/2017	Scan expiration date:	09/04/2017

Part 2. Component Compliance Summary

IP Address: 23.21.234.122	PASS
---------------------------	-------------

Part 3. Special Notes by IP Address

IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
23.21.234.122	Due to increased risk to the cardholder data environment when embedded links redirect traffic to domains outside the merchant's CDE scope, 1) confirm that this code is obtained from a trusted source, that the embedded links redirect to a trusted source, and that the code is implemented securely, or 2) confirm that the code has been removed. Consult your ASV if you have questions about this Special Note.	150010 - External Links Discovered (Web ..)	Yes	These links are hosting read-only documentation and information that is publicly available. Anytime secure data is to be accessed, a login is required.