ControlSolid

Penetration Test Attestation Letter

September 18, 2026

Provider: ControlSolid LLC **Client: Northstar Demo, Inc. (fictional)**

This fictional sample describes a hypothetical ControlSolid assessment of a payment checkout application and LLM support agent. The example assumes a non-production environment using synthetic test data only.

Scope

Scope covered checkout, APIs and webhooks, access controls, and the agent's handling of untrusted content and refund tools. The payment processor and production systems were excluded.

Standards

PCI DSS v4.0.1, Requirement 11.4: "External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected."

PCI Secure Software Standard v2.0, Requirement 10-1: "The software is designed and updated as needed to mitigate known threats and vulnerabilities that could pose risks to sensitive assets."

OWASP: Web/API references are WSTG v4.2, Web Top 10:2025, and API Top 10:2023. AI references are the GenAI LLM and Agentic Top 10, 2026 editions. These guide scope, not exhaustive coverage.

Illustrative result

The fictional test found an indirect prompt-injection path that led the agent to prepare a cross-tenant refund action. The payment API blocked execution; the issue was fixed and retested. No refund occurred.

Limitation

This scoped test alone does not establish PCI DSS compliance or satisfy every Requirement 11.4 obligation. PCI Secure Software validation is a separate assessment by a qualified Secure Software Assessor. This sample is not an ROV, AOV, or compliance opinion.